Anti-Virus™

The Virus Detection and Removal Component of iSecurity

User Manual

Version 6.3

RAZ-LEE™

The iSeries Security Experts

Updated: 02/02/2012

Copyright Notice

© Copyright Raz-Lee Security Inc. All rights reserved.

This document is provided by Raz-Lee Security for information purposes only.

Raz-Lee Security© is a registered trademark of Raz-Lee Security Inc. Action, System Control, User Management, Assessment, Firewall, Screen, Password, Audit, Capture, View, Visualizer, FileScope, Anti-Virus, AP-Journal © are trademarks of Raz-Lee Security Inc. Other brand and product names are trademarks or registered trademarks of the respective holders. Microsoft Windows© is a registered trademark of the Microsoft Corporation. Adobe Acrobat© is a registered trademark of Adobe Systems Incorporated. Information in this document is subject to change without any prior notice.

The software described in this document is provided under Raz-Lee's license agreement.

This document may be used only in accordance with the terms of the license agreement. The software may be used only with accordance with the license agreement purchased by the user. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to: photocopying, recording, or information recording and retrieval systems, without written permission given by Raz-Lee Security Inc.

Visit our website at http://www.razlee.com .

Record your Product Authorization Code Here:

Computer Model:	
Serial Number:	
Authorization Code	

TOC

Table of Contents

About This Manual 1
Product Documentation Overview 1
Printed Materials 1
Online Help 1
Typography Conventions 1
Other iSecurity Products 2

Chapter 1: Introducing Anti-Virus 4
New Features 4
Why You Need Anti-Virus 5
What are Viruses? 6
Fighting Viruses 6
Mail Scan 6
Keeping Your Computer Virus-Free 7
Feature Overview 7
Benefits 8
System Requirements 8
Native OS/400 Text Based User Interface 8
Menus 8
Data Entry Screens 9

Chapter 2: Working with PC-Type Viruses 10
Refreshing (Updating) Virus Definition Files 10
Refreshing Viruses from the CD 11
Refreshing Viruses from the Internet 12
Virus Refreshing from a LAN 13
Activating Real-Time Virus Protection 14
De-activating Real-Time Virus Protection 16
Scanning for Viruses 16
Scan Viruses 17
Quarantining Viruses 19
Scheduling Virus Scans 20
Excluding Directories During Virus Scans 22
Include Directories During Virus Scans 23
Mail Scanning 25
Anti-Virus at a Glance (PC-Type Viruses) 26

Chapter 3: Native AS/400 Suspicious Objects 27
Suspicious Native Objects 27
Scanning for Suspicious Objects 28
Scheduling Future Scans 29
Working with Suspicious Objects 29

Working with Quarantined Objects 32
Creating Reports 33
Creating Reports on Suspicious Objects 33
Creating Reports on all Non-Confirmed Objects 34
Creating Reports on all Confirmed Objects 34
Create Reports on all Quarantined Objects 34
Anti-Virus at a Glance (Native Objects) 35

Chapter 4: System Configuration 36
General Definitions 36
On Access Definitions 38
Enable SIEM & MAIL Alerting 40
SYSLOG Definitions 40
SNMP Definitions 42
Twitter Definitions 42

Appendix: License Agreement A-1
Preamble A-1
GNU LESSER GENERAL PUBLIC LICENSE A-2

About This Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on AS400 systems. However, any user with basic knowledge of AS400 operations will be able to make full use of this product after reading this book.

Product Documentation Overview

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal AS400 experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

Printed Materials

This user guide is the only printed documentation necessary for understanding this product. It is available in user-friendly PDF format and may be displayed or printed using Adobe Acrobat Reader version 4.0 or higher. Acrobat Reader is included on the product CD-ROM.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Online Help

AS400 context sensitive help is available at any time by pressing the **F1** key. A help window appears containing explanatory text that relates to the function or option currently in use. Online help will shortly be available in Windows help format for viewing on a PC with terminal emulation.

Typography Conventions

- Menu options, field names, and function key names are written in **Bold**.
- References to chapters or sections are written in *Italic*.
- OS/400 commands and system messages are written in ***Bold Italic***.
- Key combinations are separated by a dash, for example**:** Shift-Tab.
- Emphasis is written in **Times New Roman bold**.

Other iSecurity Products

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security.

Other iSecurity products include:

Assessment

Assessment checks your ports, sign-on attributes, user privileges, passwords, terminals, and more. Results are instantly provided, with a score of your current network security status with its present policy compared to the network if iSecurity were in place.

Firewall

Firewall protects and secures all types of access, to and from the System i, within or outside the organization, under all types of communication protocols. Firewall manages user profile status, secures entry via pre-defined entry points, and profiles activity by time. Its Best Fit algorithm determines the validity of any security-related action, hence significantly decreasing system burden while not compromising security.

Visualizer

Visualizer is an advanced DWH statistical tool with state-of-the-art technology. This solution provides security-related data analysis in GUI and operates on summarized files; hence, it gives immediate answers regardless of the amount of security data being accumulated.

Audit

Audit is a security auditing solution that monitors System i events in real-time. It includes a powerful query generator plus a large number of predefined reports. Audit can also trigger customized responses to security threats by means of the integrated script processor contained in Action.

Action

Action automatically intercepts and responds to security breaches, system activity events, QHST contents, and other message queues. Inquiring messages can be automatically answered. Alerts are sent by e-mail, SMS, pagers, or the message queues. Command scripts with replacement variables perform customized corrective actions, such as terminating a user session or disabling a user profile.

AP-Journal

AP-Journal automatically manages database changes by documenting and reporting exceptions made to the database journal.

View

View is a unique, patent-pending, field-level solution that hides sensitive fields and records from restricted users. This innovative solution hides credit card numbers, customer names, etc. Restricted users see asterisks or zeros instead of real values. View requires no change in existing applications. It works for both SQL and traditional I/O.

Capture

Capture silently captures and documents user screens for tracking and monitoring, without any effects on system performance. It also preserves job logs for subsequent review. Capture can run in playback mode and can be used to search within texts.

Screen

Screen protects unattended terminals and PC workstations from unauthorized use. It provides adjustable, terminal- and user-specific timeout capabilities.

Password

Password provides a first-tier wall of defense for users by ensuring that user passwords cannot be easily cracked.

Chapter 1: Introducing Anti-Virus

Raz-Lee Security's Anti-Virus module, part of the iSecurity suite, offers total protection for the System i against viruses, Trojan horses, and malicious code. Anti-Virus scans all accessed files, offers comprehensive virus detection by marking, quarantining and deleting infected files, and prevents your System i from becoming a source of infection. No effective security policy is complete without Anti-Virus.

New Features

Version 6.3

- SIEM Alerts now support both SNMP and Twitter (in addition to Syslog and email).
- Free version with permanent authorization code
  - Virus and Trojan horse protection
  - Automatic signature updates
  - Virus scanning (automatic/manual)

Version 6.0

Compatible from V5R4 - uses new ClamAV 0.97.3 engine features

- Heuristic improvements: improve the PE heuristics detection engine by adding support of bogus icons and fake PE header information. In a nutshell, ClamAV can now detect malware that tries to disguise itself as a harmless application by using the most common Windows program icons.
- Signature Improvements: logical signature improvements to allow more detailed matching and referencing groups of signatures. Additionally, improvements to wildcard matching on word boundaries and newlines.
- Support for new archives: 7zip, InstallShield and CPIO. LibClamAV can now transparently unpack and inspect their contents.
- Support for new executable file formats: 64-bit ELF files and OS X Universal Binaries with Mach-O files. Additionally, the PE module can now decompress and inspect executables packed with UPX 3.0.
- New PDF parser
  - Support for custom database URLs
  - Support for signatures based on SHA1 and SHA256
  - Better error detection
  - Performance improvements: overall performance improvements and memory optimizations for a better overall resource utilization experience.

Version 5.8

- When scanning only new (not scanned before) files, the scan check is done in the context of the same job, which saves the overhead of opening a new job. In addition, it saves locking problem in one of SEA customers.
- When ending all subsystems by ENDSBS *ALL *IMMED, for backup as example, the scan exit programs are removed automatically, to avoid IFS hang-up.

In every directory scan, there is a heading with time and name of the directory scanned.

Version 5.6:

- Includes the current new version of ClamAV: 0.95.3 (AV5.5 was 0.95.2)
- Fix of restart bug when previous jobs are not terminated.
- Remove Scan exit points when ending ZANTIVIRUS subsystem and avoid hang-up in IPL process

Version 5.5:

- Check for PASE installation before installing the product.
- Add STRSEC to support product authorization.

Version 5.2:

- Phishing email detection - good for mail servers.
- Alarm print when virus database is older than 7 days.
- Works faster in PASE (Linux like) mode.
- Support for sending real-time virus alerts to SYSLOG, QSYSOPR and e-mails.

Version 4.5:

- Define general syslog usage in Anti-Virus option 81 -> 21.
- New options in Anti-Virus "On Access" Definitions menu 81->2.

Why You Need Anti-Virus

Until just a few years ago, the System i was used almost exclusively in a closed environment, and the OS/400 operating system provided the strongest data and system security in the world. But times have changed. In today's world of PCs, distributed databases, the Internet and web technologies, closed computing environments are nearly extinct. Technological advances opened up the System i to the rest of the world, but in the process, brought with it many of the security risks inherent in distributed environments, leading to a shocking discovery. Although the System i AS/400 doesn't run .exe files, it can house virus-infected files–so they can wait, silent and deadly, until someone on the network transfers and opens the relevant file on their PC.

What are Viruses?

Viruses are programs or pieces of malicious code that load and attach themselves to your computer without your knowledge. Once inside, they infect .exe files and disk boot sectors, where they proceed to replicate at enormous speeds. Viruses are all man-made. They range from harmless pranks that are mere annoyances to your computer, such as screen messages, to catastrophic instruments of destruction that can wipe out your hard disk.

There are different types of viruses. Worms are special kinds of viruses that replicate themselves but cannot attach to other programs. Trojan horses, named after the classic Greek myth, also do not replicate themselves. They are programs that pretend to have useful and helpful features, while they are actually destructive. Malware (malicious software) is actually a general, all-encompassing term for any program designed to "take over" and harm your computer and operating system.

In history, the Trojan horse was a large hollow wooden horse that was filled with Greek soldiers. After the horse was introduced within the walls of Troy, the soldiers climbed out of the horse and fought the Trojans. In the computer world, a program that hides destructive functions is often called a Trojan horse.

Fighting Viruses

New viruses are constantly being introduced to the world. The good news is that there are solid tools that follow every new threat and enable you to keep your computer and network clean, safe, and virus-free. But standard, PC-based anti-virus programs are simply not effective enough in the AS/400 world. When checking the Integrated File System, they're slow, can compromise security, and are not immune to viruses themselves.

The answer is a native, AS/400-based application. By using Clam™ anti-virus detection technology, Raz-Lee's Anti-Virus enables you to fight viruses using a comprehensive and specially designed product. Working extremely fast, Anti-Virus' user-friendly interface incorporates the most intuitive activation features on the market, helping you to keep viruses away from your network and PC.

Mail Scan

Anti-Virus takes control just when the IFS file that contains an email is being closed or opened. That way, the scan is done before the recipient gets the email. If the email is a phishing mail or contains a virus, the recipient gets a mail describing the virus found and name of the quarantined file - the recipient will never get the actual infected email. Phishing mail scan is done only by ClamAV.

Keeping Your Computer Virus-Free

In addition to installing Raz-Lee's Anti-Virus, and updating virus definitions on a regular basis, it is important to note that no single product can completely eliminate the virus threat. It is mandatory to take additional precautions in order to safeguard your network:

- Inform all personnel at your company of the dangers of virus infection. Train them to recognize the signs of possible infection. These include error messages, corrupt data and system slowdown.
- Maintain reliable data backups at all times, i.e. CDs, additional hard disks, etc.
- Do not open any e-mail attachment unless you know it is from a reliable source. Attachments are notorious for spreading viruses.
- Be suspicious of e-mails with over-general message lines, such as "RE: An Answer", "Thanks", or "Hi."
- Do not open any attachments with file extensions such as .drv, .sys, .dll, .exe, .eml, .scr, .ocx, .com, .pif, .bin, .vbe, .bat, .nws, l.nk, .cpl, and .shs.
- Choose assistants to assist you in handling emergencies and possible infection if the systems administrator isn't present.

Feature Overview

- Automatic, regularly updated database
- Mail Support for SMTP mail servers, that scans and sends alarm to the recipient instead of the original infected mail
- Detects, catches, and quarantines viruses, worms, Trojan horses, and malicious software (malware)
- Command-line scanner
- Database updater with support for digital signatures
- Cannot be disabled by viruses
- On-Access and Scanning
- Built-in support for zip, gzip, jar, and tar files
- User-friendly, multilingual interface (green screen and GUI) with simple activation features
- Integration with OS/400 Scheduler
- Summary Log for review and analysis.

Benefits

- Prevents your System i from becoming an infection source
- Scans files before and/or after they are used
- Built-in scheduler enables planned virus scanning
- Based on a popular signature file used in the Open Source (Linux) environment
- Signature file is updated often - even before some of the commercial files
- Signature file loaded directly from the web into the System i or from a web-connected PC which disconnects from the web upon System i access
- User-friendly green-screen and GUI interfaces.

System Requirements

- Disk space: 110MB
- **PASE** (Linux-like environment) installation: required
- Operating System: V5R4 or higher.

NOTE: *PASE installation will be required in the near future for Audit, FIleScope and perhaps for other tools as well.*

Native OS/400 Text Based User Interface

Anti-Virus is designed to be a user-friendly product. The user interface follows standard System i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Menus

Product menus allow for easy access to all features with a minimum of keystrokes. Menu option numbering and terminology are consistent throughout this product as well as other Raz-Lee products. To select a menu option, simply type the option number and press Enter. The command line is available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press F10 to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support.

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press **Enter** or **Field Exit**
- To move from one field to another without changing the contents press **Tab**
- To view options for a data field together with an explanation, press **F4**
- To accept the data displayed on the screen and continue, press **Enter.**

The following function keys may appear on data entry screens.

Function Key	Description
F1 - Help	Display context-sensitive help
F3 - Exit	End the current task and return to the screen or menu from which the task was initiated
F4 - Prompt	Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
F6 - Add New	Create a new record or data item
F8 - Print	Print the current report or data item
F9 - Retrieve	Retrieve the previously-entered command
F12 - Cancel	Return to the previous screen or menu without updating

Chapter 2: Working with PC-Type Viruses

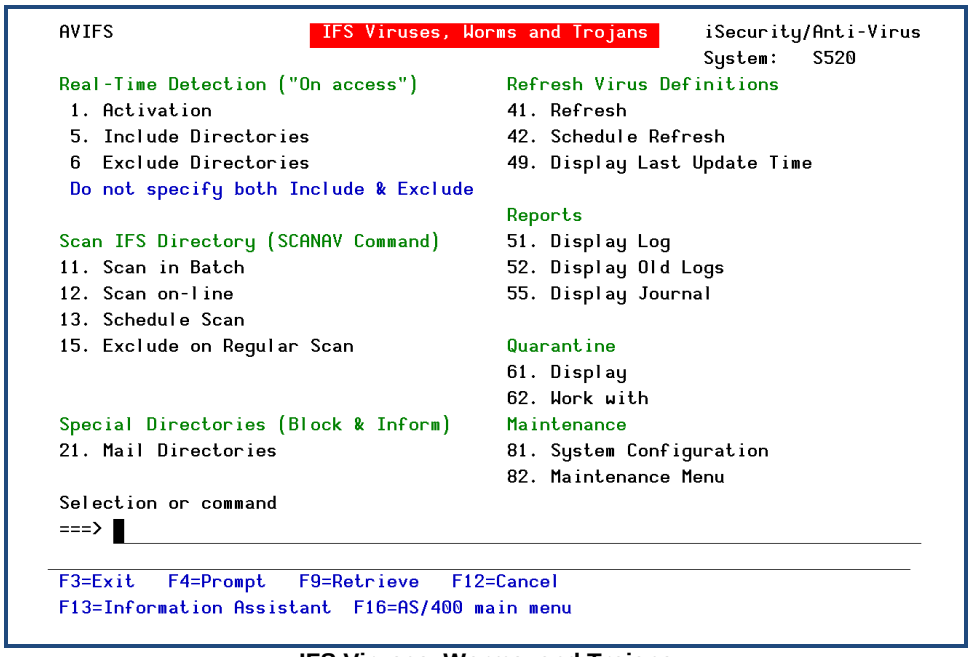
This chapter guides you through the steps necessary to begin using **Authority on Demand** for the first time. Also covered in this chapter are the basic procedures for configuring the product for day-to-day use.

This chapter describes the procedures for setting up real-time detection and anti-virus activation.

Type ***STRSEC*** on any command line and select option **5. Anti-Virus**.

> **NOTE:** *If system password is requested, type QSECOFR*

To work with PC-type viruses, worms, and Trojan horses, select **11. IFS Viruses, Worms and Trojans** from the main menu.



IFS Viruses, Worms, and Trojans

Refreshing (Updating) Virus Definition Files

Perform this procedure to ensure that you have the most up-to-date virus definition files available (virus definitions are generally updated on average twice daily). Anti-Virus provides two options for updating. Both are accessed by selecting **11. IFS Viruses, Worms and Trojans > 41. Refresh**.

- This sub-menu has an extended option, ***CD**. This option refreshes the Virus Signature Database from a CD which was burned using the internet-connected PC which downloaded files main.cvd and daily.cvd from the ClamAV server.

- The option ***INTERNET** is downloaded directly from the internet to the System i. This option enables users to refresh virus definitions at their own computers.
- The option ***LAN** is first download first to a PC, then uploaded to the System i via a LAN. This option enables only one user to download definitions, thereby providing greater security. All other users receive their updates from that user.

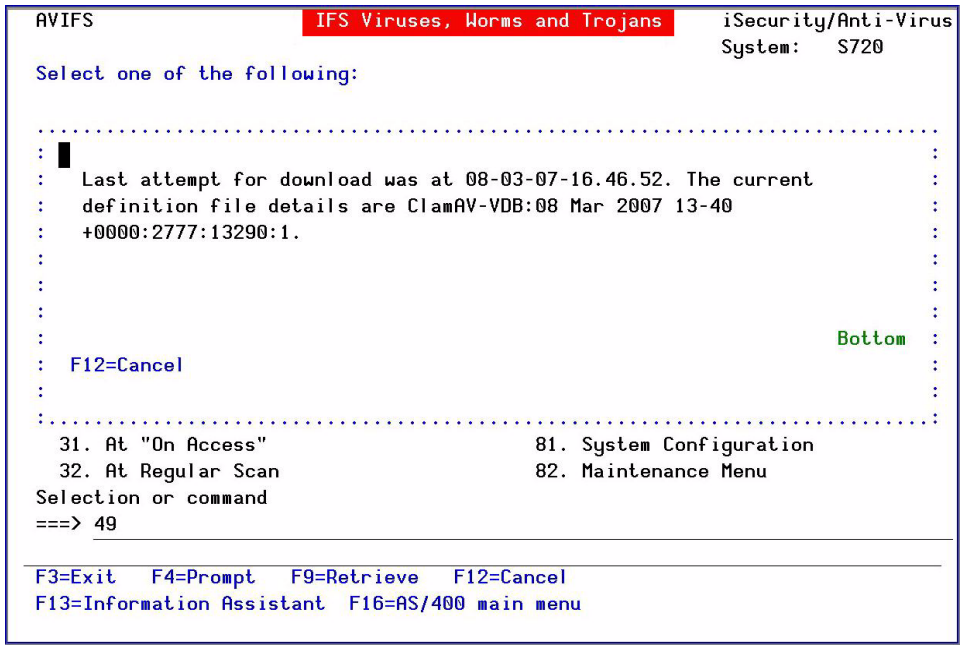
NOTE: *Since many System i computers are not permitted to be directly connected to the internet because of regulatory issues, we recommend using option ***CD** instead.*

Each procedure is explained below in detail.

Refreshing Viruses from the CD

1. Enter the command ***STRAV*** to return to the **Anti-Virus** main screen.
2. Select **41. Refresh**. The **Update Virus Definitions (UPDAVDFN)** screen appears.
3. Select ***CD** from the **Type** field and press **Enter**. A message screen appears after a few moments with update details.
4. Press **Enter** to return to the main screen.

NOTE: *To view the most recent update, select* **49. Display Last Update Time**. *The date appears together with the precise update time and file definition file details. The following shows a sample message (this step is also relevant for internet and LAN refreshing).*



Display Last Update Time

Refreshing Viruses from the Internet

NOTE: *Steps 1 and 2 are to be performed only when updating virus definitions for the first time.*

1. Enter the command ***CFGTCP*** into the command line and select option **12**. The **Change TCP/IP Domain (CHGTCPDMN)** screen appears.
2. Check that your DNS (Domain Name Server) is defined. If not, update your ISP Domain details.
3. Press **Enter** and then ***STRAV*** to return to the **Anti-Virus** main screen.
4. Select **41. Refresh**. The **Update Virus Definitions (UPDAVDFN)** screen appears.

NOTE: Select ***INTERNET** from the **Type** field and press **Enter**. A message screen appears after a few moments with update details.

6. Press **Enter** to return to the main screen.

Virus Refreshing from a LAN

> **NOTE:** *Steps 1 - 9 are to be performed only when updating virus definitions for the first time.*

1. Enter the command ***CFGTCP*** into the command line and select option **10**. The **Work with TCP/IP Host Table Entries** screen appears.
2. Add your IP address with the host name ***AVDBPC*** by using option **1** next to the blank line at the top of the **Internet Address** column.
3. Copy directory ***avpc*** from the installation disk to ***C:***\.
4. Open folder ***C:\avpc*** and double-click Apache installation file: ***C:\avpc\apache_2.0.43-win32-x86-no_ssl.exe***.

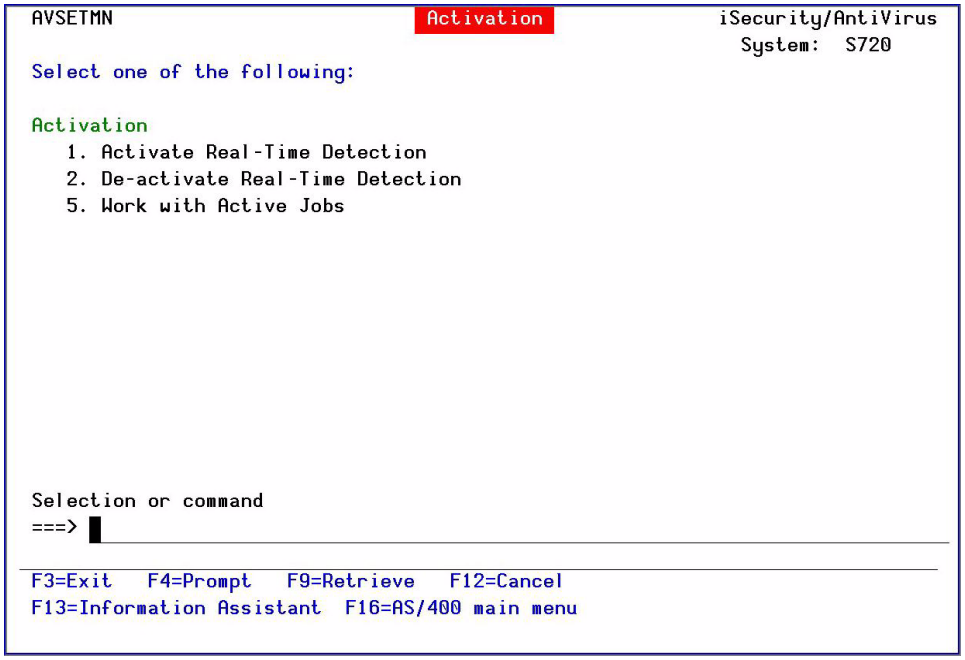
> **NOTE:** *Enter domain, server name, and email when prompted (you can use any text you like).*

6. Double-click batch file: ***ScheduledUpdate.bat***. When the download is finished, files are ready for the AS/400 update tool.
7. To update virus database on a daily basis, add ***ScheduledUpdate.bat*** to the PC scheduled tasks. Select **Start > Programs > Accessories > System Tools > Scheduled Tasks**, and click **Add Scheduled Task**.
8. Browse to folder ***C:\avpc*** and open ***ScheduledUpdate.bat***.
9. Check daily option, fill in login password, choose your preferred time for the update, select **Finish**, and press **Enter**.
10. Return to native interface and enter ***STRAV*** to return to the **Anti-Virus** main screen.
11. Select **41. Refresh**. The **Update Virus Definitions (UPDAVDFN)** screen appears.
12. Select ***LAN** from the **Type** field and press **Enter** to begin the update process.
13. Press **Enter** to return to the main screen.

Activating Real-Time Virus Protection

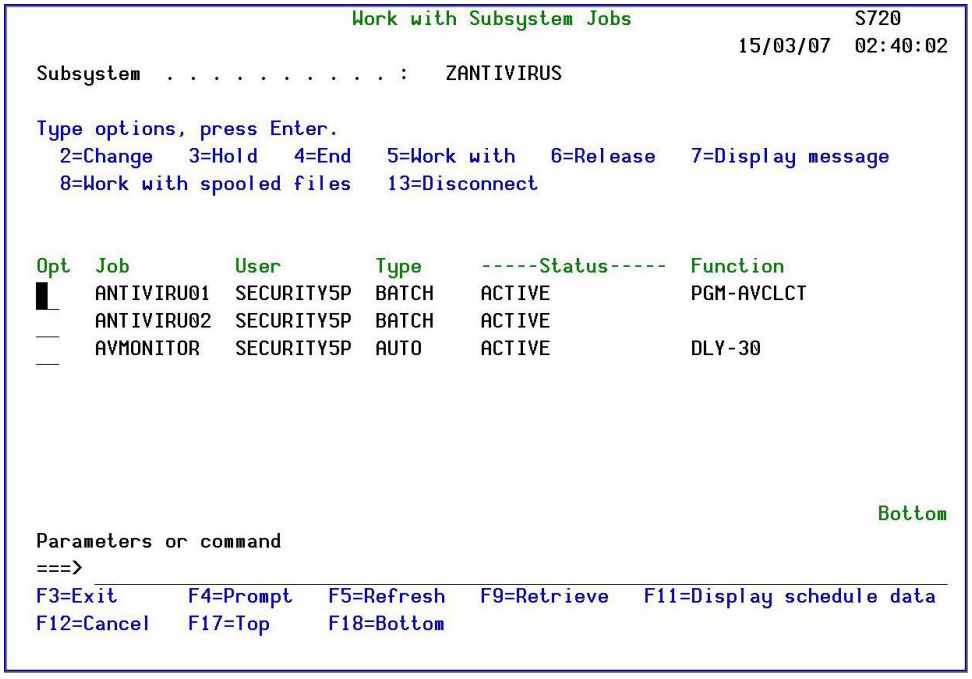
This feature enables Anti-Virus to get "up and running" and start examining all incoming files, folders, and IFS objects. To activate real-time detection, follow this procedure.

1. Select **1. Activation**. The **Activation** screen appears.



Activation

2. Select **1. Activate Real-Time Detection** from the **Activation** menu.
3. Check that the subsystem, **ZANTIVIRUS**, is activated by selecting **5. Work with Active Jobs** from the **Activation** menu. The **Work with Subsystem Jobs** screen appears.
4. Check that the word **ACTIVE** appears in the **Status** field as shown in the following screen capture. If so, the subsystem is activated that **Anti-Virus** is already providing top virus protection and removal.


Work with Subsystem Jobs
S720
15/03/07 02:40:02
Subsystem . . . . . : ZANTIVIRUS
Type options, press Enter.
2=Change 3=Hold 4=End 5=Work with 6=Release 7=Display message
8=Work with spooled files 13=Disconnect
Opt Job User Type -----Status----- Function
ANTIVIRU01 SECURITY5P BATCH ACTIVE PGM-AVCLCT
ANTIVIRU02 SECURITY5P BATCH ACTIVE
AVMONITOR SECURITY5P AUTO ACTIVE DLY-30
Bottom
Parameters or command
===>
F3=Exit F4=Prompt F5=Refresh F9=Retrieve F11=Display schedule data
F12=Cancel F17=Top F18=Bottom

Work with Subsystem Jobs (ZANTIVIRUS Active)

NOTE: *The **Anti-Virus** subsystem is composed of three processes (jobs). To work with these processes, select* **Option 5**.

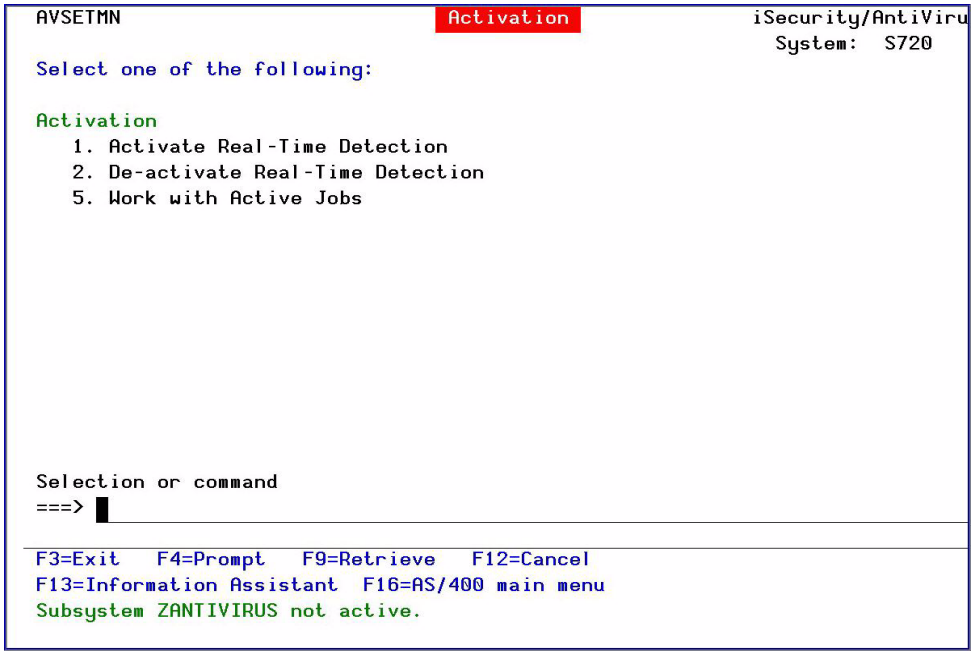
6. Press **F12** to return to the **Activation** menu.

NOTE: *Users are alerted regarding viruses found through the* **Real-Time Detection** *feature only when they try to open the file containing the virus. In this case, access is denied to the file and an Attribute (Scan/Fail message) appears in the log file. Consequentially, the virus contained in the file can do no further harm.*

NOTE: *The command **SMZV/ENDRTAV** stops accepting new objects to be checked and lets the current object being checked to be finished, then the subsystem ZANTIVIRUS ends. The command **SMZV/STRRTAV** starts the system.*

De-activating Real-Time Virus Protection

1. To de-activate real-time detection, select **2. De-activate Real-Time Detection** from the **Activation** menu.
2. To check that the subsystem is de-activated, wait about 30 seconds and select **5. Work with Active Jobs**. A message should appear at the bottom of the **Activation** screen as shown in the following screen capture.



Work with Subsystem Jobs (Subsystem ZANTIVIRUS Not Active)

Scanning for Viruses

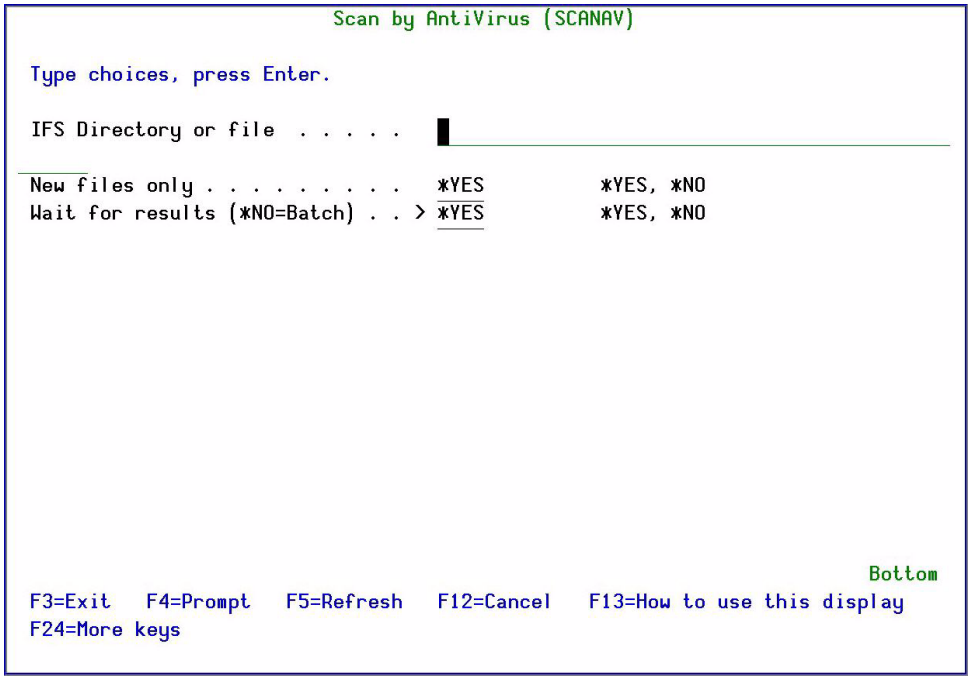
Anti-Virus supports two different types of virus scans:

- **Scan in Batch** (**Opt 11**) - This option enables **Anti-Virus** scanning to run as a background process, thus enabling you to continue working in another application. At the end of the scan, you must select **51. Display Log** to see results.
- **Scan Now** (**Opt 12**) - This option creates an interactive process, enabling you to view the Log as the files are being scanned.

Scan Viruses

To perform virus scans, follow this simple procedure.

1. Select **11. Scan** or **12. Scan Now** from the main menu. The **Scan by Anti-Virus** screen appears. An explanatory table follows the screen capture.


Scan by AntiVirus (SCANAV)
Type choices, press Enter.
IFS Directory or file . . . . .
New files only . . . . . *YES *YES, *NO
Wait for results (*NO=Batch) . . > *YES *YES, *NO
Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

Scan by Anti-Virus (SCANAV)

Option	Description
IFS Directory or file	Name of directory or name of file
New Files Only *	***YES** = Scan only those files that have been added since the previous scan ***NO** = Scan all files in IFS
Wait for results	***YES** = Performs on-line scan ***NO** = Performs batch scan

2. Enter the file name or directory you want to scan plus additional parameters, and press **Enter**. A summary scan appears at the scan finish. Any virus found is immediately quarantined.
3. To abort a scan *after* scanning has begun, select **2. De-activate Real-Time Detection** from the **Activation** menu.

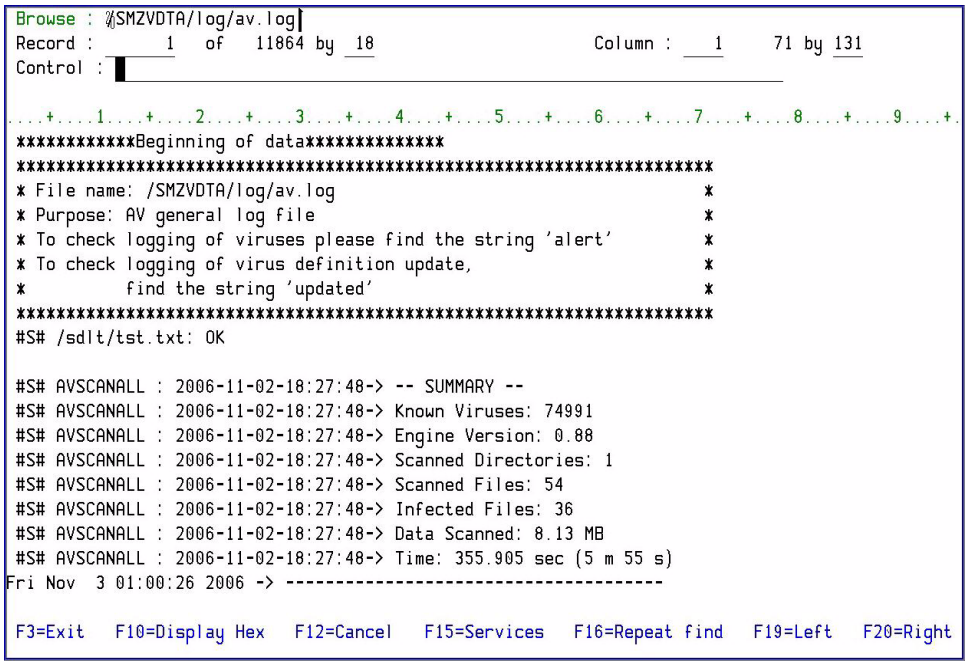
4. Check **Anti-Virus**' virus-fighting capabilities by scanning "false" and harmless files. **Anti-Virus** will consider it a virus and place it in quarantine. If not, check your configuration settings and/or contact Raz-Lee. The files names are ***eicar.com*** and ***MyDoomS***, both found in ***/SMZVDTA/virus_template***.

NOTE: *If you are using the* **Scan in Batch** *option (**11**), you must select* **51. Display Log** *from the main menu to see virus details at the end of the scan (use* **Page Down** *on the keyboard if necessary).*

NOTE: *This step is not necessary for real-time scans, as results are displayed immediately without any user prompting. The summary log offers this information:*

- *Known viruses*
- *Scanned directories*
- *Scanned files*
- *Infected files*
- *Data scanned*
- *I/O buffer size*
- *Time (of scan)*
- *Starting time of scan*
- *Virus scans*
- *Quarantined viruses*
- *Real-time activation/de-activation*
- *Virus removal*
- *Virus definition updates*
- *Scan scheduling.*

The following is an example of a summary log.

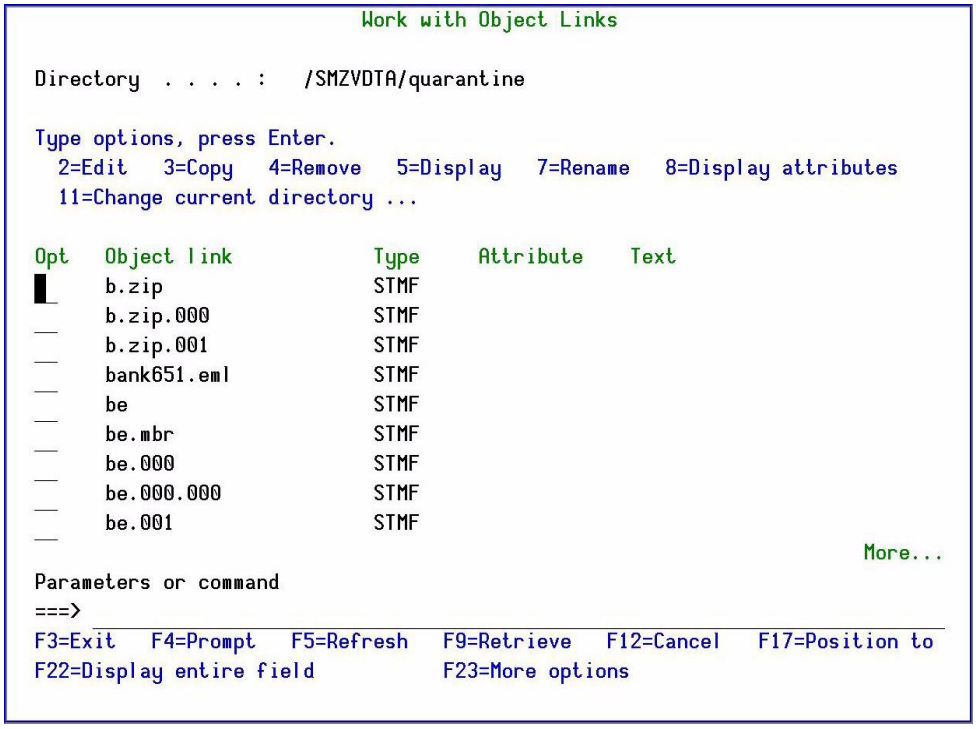

Browse : /SMZVDTA/log/av.log
Record : 1 of 11864 by 18 Column : 1 71 by 131
Control :
...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+.
**********Beginning of data**********
* File name: /SMZVDTA/log/av.log *
* Purpose: AV general log file *
* To check logging of viruses please find the string 'alert' *
* To check logging of virus definition update, *
* find the string 'updated' *
#S# /sdlt/tst.txt: OK
#S# AVSCANALL : 2006-11-02-18:27:48-> -- SUMMARY --
#S# AVSCANALL : 2006-11-02-18:27:48-> Known Viruses: 74991
#S# AVSCANALL : 2006-11-02-18:27:48-> Engine Version: 0.88
#S# AVSCANALL : 2006-11-02-18:27:48-> Scanned Directories: 1
#S# AVSCANALL : 2006-11-02-18:27:48-> Scanned Files: 54
#S# AVSCANALL : 2006-11-02-18:27:48-> Infected Files: 36
#S# AVSCANALL : 2006-11-02-18:27:48-> Data Scanned: 8.13 MB
#S# AVSCANALL : 2006-11-02-18:27:48-> Time: 355.905 sec (5 m 55 s)
Fri Nov 3 01:00:26 2006 -> ----------
F3=Exit F10=Display Hex F12=Cancel F15=Services F16=Repeat find F19=Left F20=Right

Summary Log (showing scan details)

Quarantining Viruses

Quarantine is a secure, isolated location which contains viruses that infect your files. Viruses that have been placed in Quarantine can do no further harm (V5R3 and up); they can neither replicate themselves nor infect other files. Once inside Quarantine, an infected file can be kept there indefinitely, erased completely or returned to its location.

1. To view virus quarantine details, select **61. Display**. The **Display Object Links** screen appears.
2. Choose **5. Display**. Use the **Page Down** option on the keyboard to view additional details.
3. To delete a file, select **62. Work With**. The **Work with Object Links** screen appears.



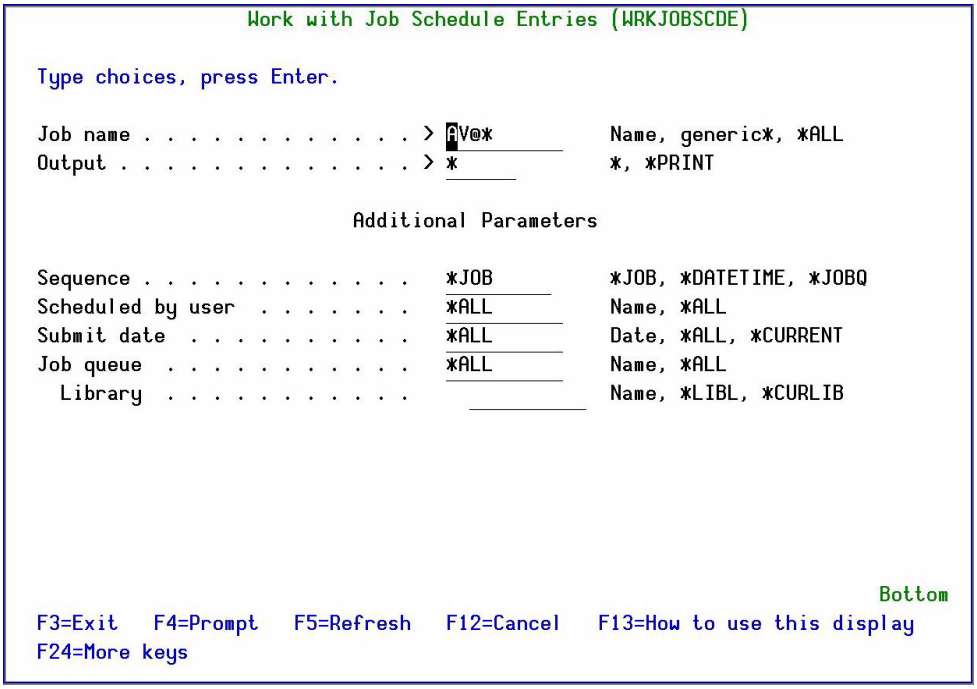
Work with Object Links

4. To remove a virus from quarantine, and thereby erase it, select **Opt 4**, and then **Enter** to confirm.

Scheduling Virus Scans

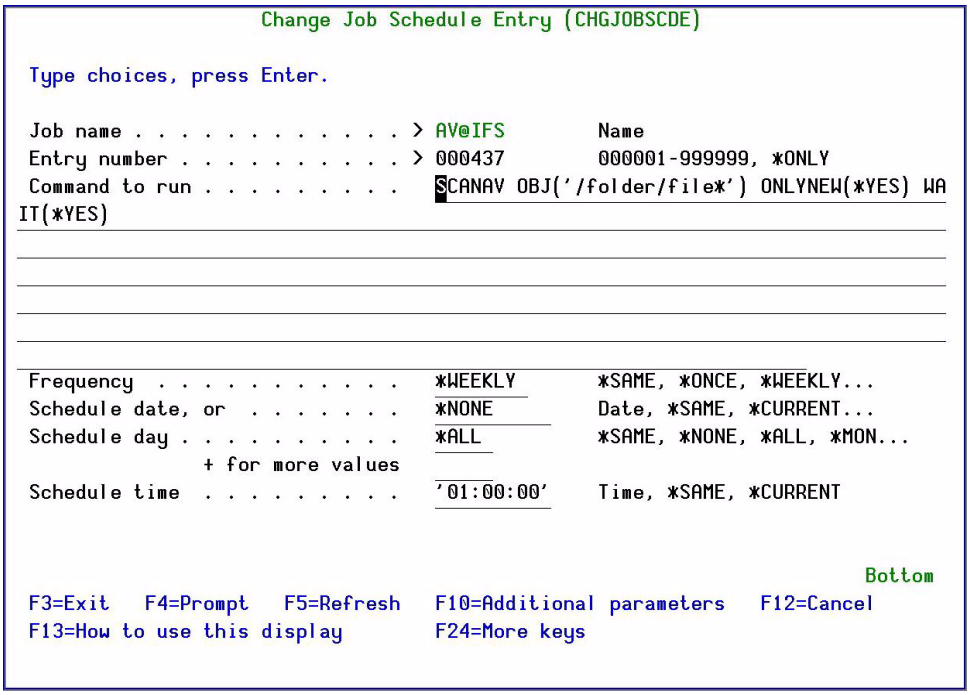
Use this option to schedule a regularly-occurring scan, i.e. 9:00 every morning, or a single, specific scan to occur at a future time.

1. Select **13. Schedule Scan**. The **Work with Job Schedule Entries (WRKJOBSCDE)** screen appears.


Work with Job Schedule Entries (WRKJOBSCDE)
Type choices, press Enter.
Job name . . . . . > QV@*
Name, generic*, *ALL
Output . . . . . > *
*, *PRINT
Additional Parameters
Sequence . . . . . *JOB
*JOB, *DATETIME, *JOBQ
Scheduled by user . . . . . *ALL
Name, *ALL
Submit date . . . . . *ALL
Date, *ALL, *CURRENT
Job queue . . . . . *ALL
Name, *ALL
Library . . . . . Name, *LIBL, *CURLIB
Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys

Work with Job Schedule Entries (WRKJOBSCDE)

2. Press **Enter**. The screen shows a list of defined jobs.
3. Type **2** in the **Opt** field to modify an existing job (or press **F6** to add a new job) and press **Enter**. The **Change Job Schedule Entry (CHGJOBSCDE)** screen appears. The following screen shows an example.


Change Job Schedule Entry (CHGJOBSCDE)
Type choices, press Enter.
Job name . . . . . > AV@IFS Name
Entry number . . . . . > 000437 000001-999999, *ONLY
Command to run . . . . . SCANAV OBJ('/folder/file*') ONLYNEW(*YES) WAIT(*YES)
Frequency . . . . . *WEEKLY *SAME, *ONCE, *WEEKLY...
Schedule date, or . . . . . *NONE Date, *SAME, *CURRENT...
Schedule day . . . . . *ALL *SAME, *NONE, *ALL, *MON...
+ for more values
Schedule time . . . . . '01:00:00' Time, *SAME, *CURRENT
Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Change Job Schedule Entry (CHGJOBSCDE)

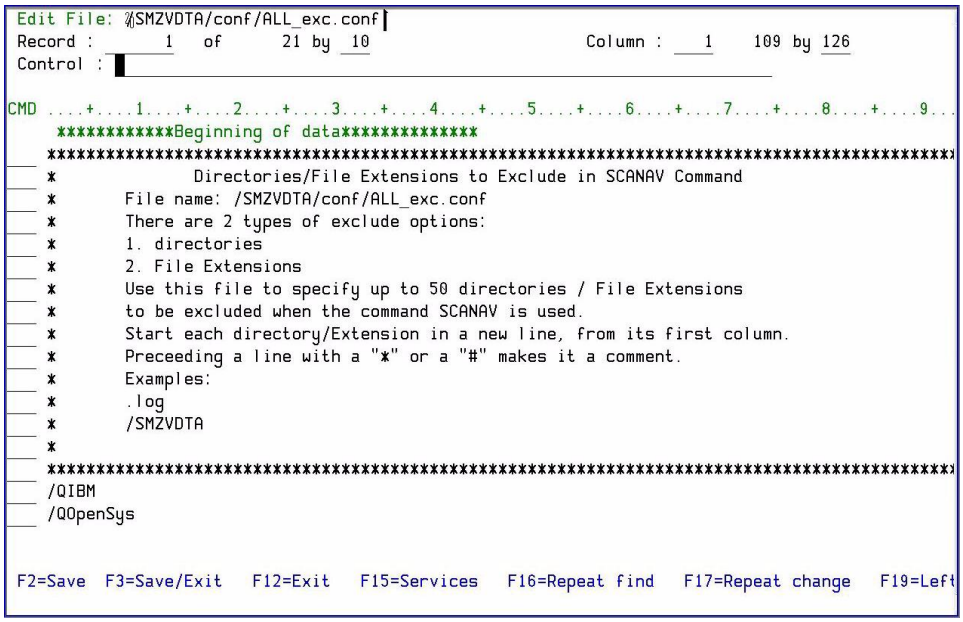
4. Enter your parameters (frequency, date, day, time) and press **Enter**.

Excluding Directories During Virus Scans

This procedure enables you to exclude up 50 file extensions and/or directories during virus scans.

- To exclude files and folders during real-time scanning, select **6. At "IFS Viruses, Worms and Trojans"**.
- To exclude files and folders during scheduled scanning, select **15. Exclude on Regular Scan**.

1. Enter file name in the **Edit File** field (see upper call out in the following screen capture).
2. Enter additional files in the field provided between the **Beginning of Data** and **End of Data** fields (see lower arrow in the following screen capture).


Edit File: /SMZVDTA/conf/ALL_exc.conf
Record : 1 of 21 by 10 Column : 1 109 by 126
Control :
CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9...
**********Beginning of data**********
* Directories/File Extensions to Exclude in SCANAV Command
* File name: /SMZVDTA/conf/ALL_exc.conf
* There are 2 types of exclude options:
* 1. directories
* 2. File Extensions
* Use this file to specify up to 50 directories / File Extensions
* to be excluded when the command SCANAV is used.
* Start each directory/Extension in a new line, from its first column.
* Preceeding a line with a "*" or a "#" makes it a comment.
* Examples:
* .log
* /SMZVDTA
*
/QIBM
/QOpenSys
F2=Save F3=Save/Exit F12=Exit F15=Services F16=Repeat find F17=Repeat change F19=Left

Exclude Directories

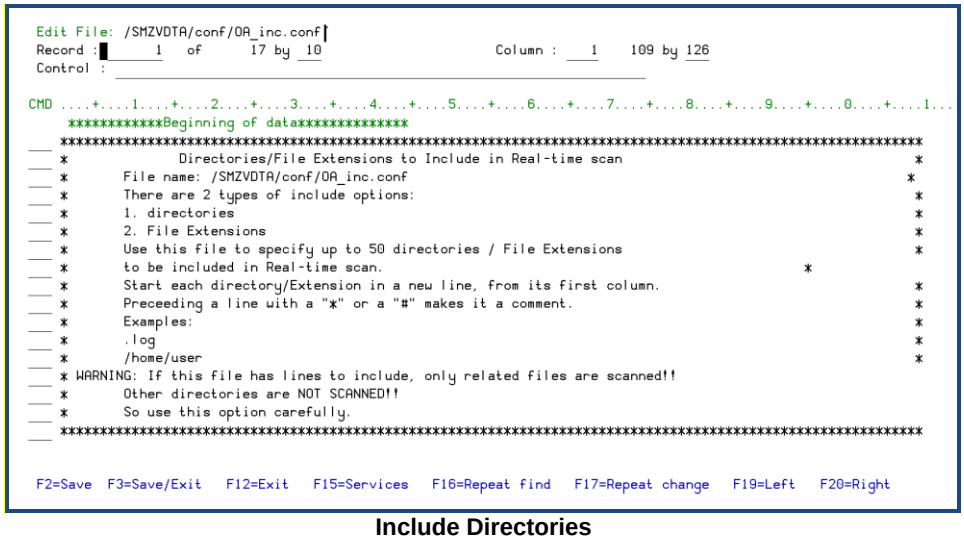
- To save without exiting, press **F2**
- To save and exit, press **F3** twice
- To exit without saving, press **F12**.

Include Directories During Virus Scans

This procedure enables you to include up 50 file extensions and/or directories during virus scans.

To include files and folders during real-time scanning, select **5. At "IFS Viruses, Worms and Trojans**".

1. Enter file name in the **Edit File** field (see upper call out in the following screen capture).
2. Enter additional files in the field provided between the **Beginning of Data** and **End of Data** fields (see lower arrow in the following screen capture).


Edit File: /SMZVDTA/conf/OA_inc.conf
Record : 1 of 17 by 10 Column : 1 109 by 126
Control :
CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1...
**********Beginning of data**********
* Directories/File Extensions to Include in Real-time scan *
* File name: /SMZVDTA/conf/OA_inc.conf *
* There are 2 types of include options: *
* 1. directories *
* 2. File Extensions *
* Use this file to specify up to 50 directories / File Extensions *
* to be included in Real-time scan. *
* Start each directory/Extension in a new line, from its first column. *
* Preceeding a line with a "*" or a "#" makes it a comment. *
* Examples: *
* .log *
* /home/user *
* WARNING: If this file has lines to include, only related files are scanned!!
* Other directories are NOT SCANNED!!
* So use this option carefully.
F2=Save F3=Save/Exit F12=Exit F15=Services F16=Repeat find F17=Repeat change F19=Left F20=Right

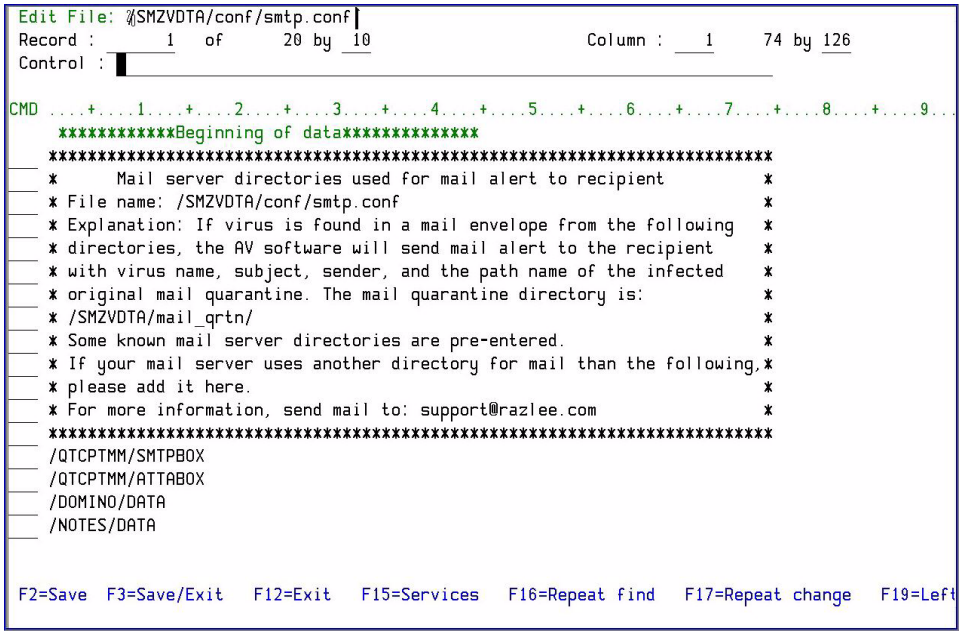
Include Directories

- To save without exiting, press **F2**
- To save and exit, press **F3** twice
- To exit without saving, press **F12**.

Mail Scanning

Anti-Virus 5.8 and higher comes with build-in Mail Alert for SMTP mail servers of:

- AS/400 build-in SMTP server
- Lotus Notes SMTP server.

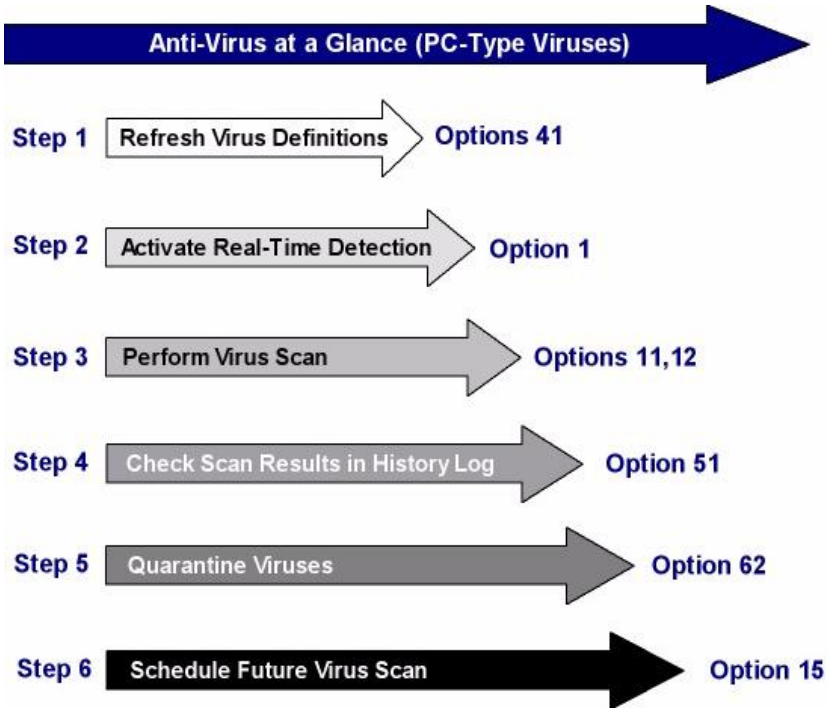

Edit File: /SMZVDTA/conf/smtp.conf
Record : 1 of 20 by 10 Column : 1 74 by 126
Control :
CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9...
**********Beginning of data**********
* Mail server directories used for mail alert to recipient *
* File name: /SMZVDTA/conf/smtp.conf *
* Explanation: If virus is found in a mail envelope from the following *
* directories, the AV software will send mail alert to the recipient *
* with virus name, subject, sender, and the path name of the infected *
* original mail quarantine. The mail quarantine directory is: *
* /SMZVDTA/mail_qrtn/ *
* Some known mail server directories are pre-entered. *
* If your mail server uses another directory for mail than the following, *
* please add it here. *
* For more information, send mail to: support@razlee.com *
/QTCPTMM/SMTPBOX
/QTCPTMM/ATTABOX
/DOMINO/DATA
/NOTES/DATA
F2=Save F3=Save/Exit F12=Exit F15=Services F16=Repeat find F17=Repeat change F19=Left

Mail Scanning

The Mail Alert scans the email received on the SMTP server and sends an alarm to the recipient instead of the original infected mail.

Anti-Virus at a Glance (PC-Type Viruses)

The following shows the basic procedures described in this chapter.



Chapter 3: Native AS/400 Suspicious Objects

This chapter will cover suspicious objects found in both the IFS and the Native AS/400. A suspicious object is that which may or may not have integrity violations. An integrity violation occurs if:

- Command has been tampered with
- Object has a digital signature that is not valid
- Object has an incorrect domain attribute for its object type
- Program or module object has been tampered with
- Library's attributes have been tampered with.

If an integrity violation has occurred, the object name, library name (or path name), object type, object owner, and type of failure are logged to a database file.

If you scan the integrated file system using a PC mapped to your system through System i NetServer, the following actions occur:

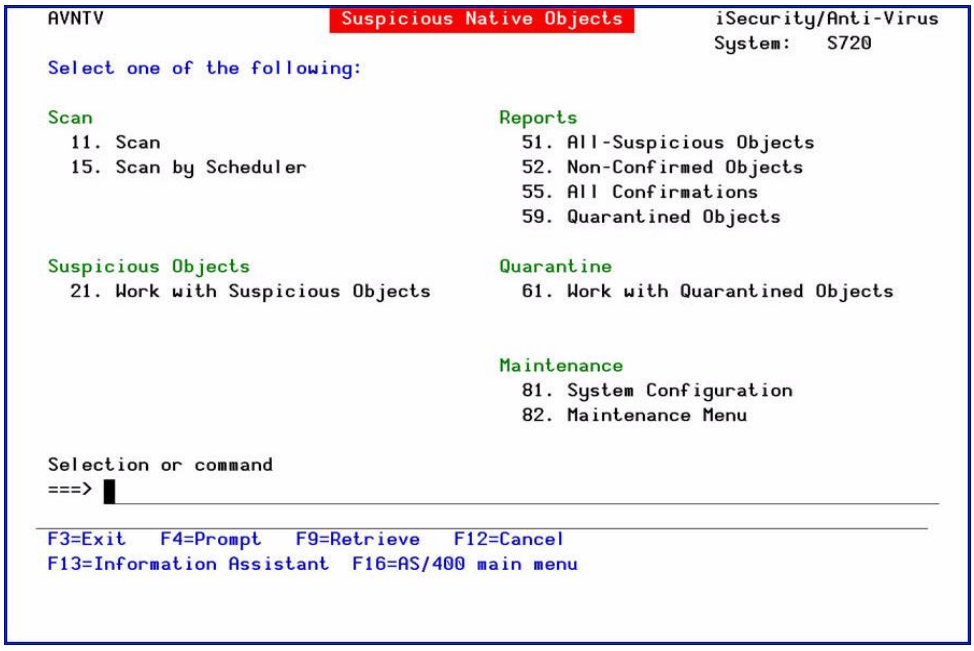
- Uses up network resources
- Moves data across the network in the clear
- Might cause scanners to go into infinite loops.

Suspicious Native Objects

Type ***STRSEC*** on any command line and select option **5. Anti-Virus**.

> **NOTE:** *If system password is requested, type* QSECOFR.

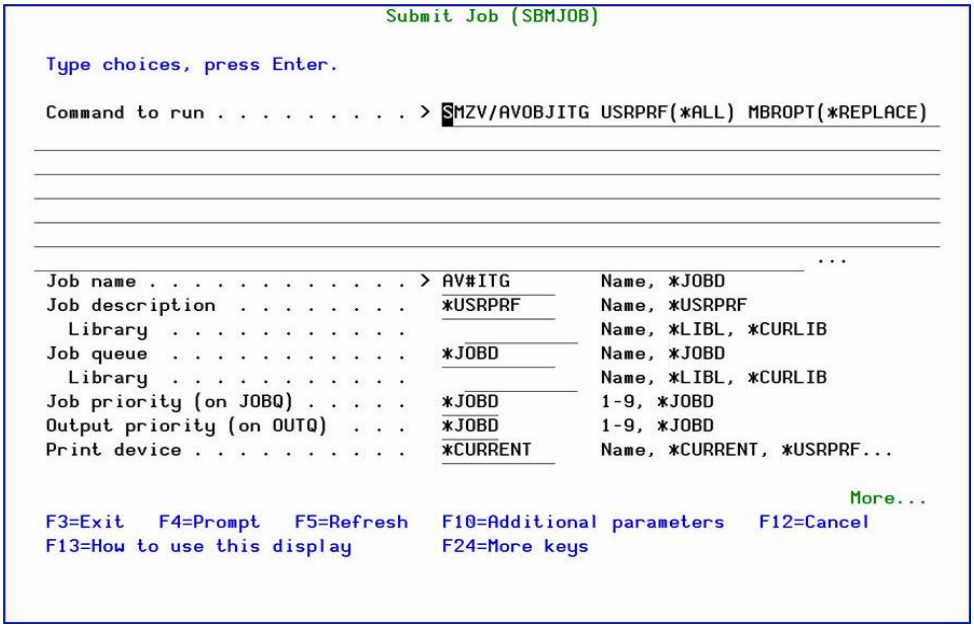
To work with Native AS/400 Suspicious Objects, select **21. Suspicious Objects** from the **Anti-Virus** main menu. The **Suspicious Native Objects** screen appears. Proceed to the next step, ***Scanning for Viruses***.



Suspicious Native Objects

Scanning for Suspicious Objects

Scan for suspicious objects by selecting **Opt 11. Scan**. The **Submit Job (SBMJOB)** screen appears.


Submit Job (SBMJOB)
Type choices, press Enter.
Command to run . . . . . > SMZV/AVOBJITG USRPRF(*ALL) MBROPT(*REPLACE)
Job name . . . . . > AV#ITG Name, *JOBD
Job description . . . . . *USRPRF Name, *USRPRF
Library . . . . . Name, *LIBL, *CURLIB
Job queue . . . . . *JOBD Name, *JOBD
Library . . . . . Name, *LIBL, *CURLIB
Job priority (on JOBQ) . . . . . *JOBD 1-9, *JOBD
Output priority (on OUTQ) . . . *JOBD 1-9, *JOBD
Print device . . . . . *CURRENT Name, *CURRENT, *USRPRF...
More...
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

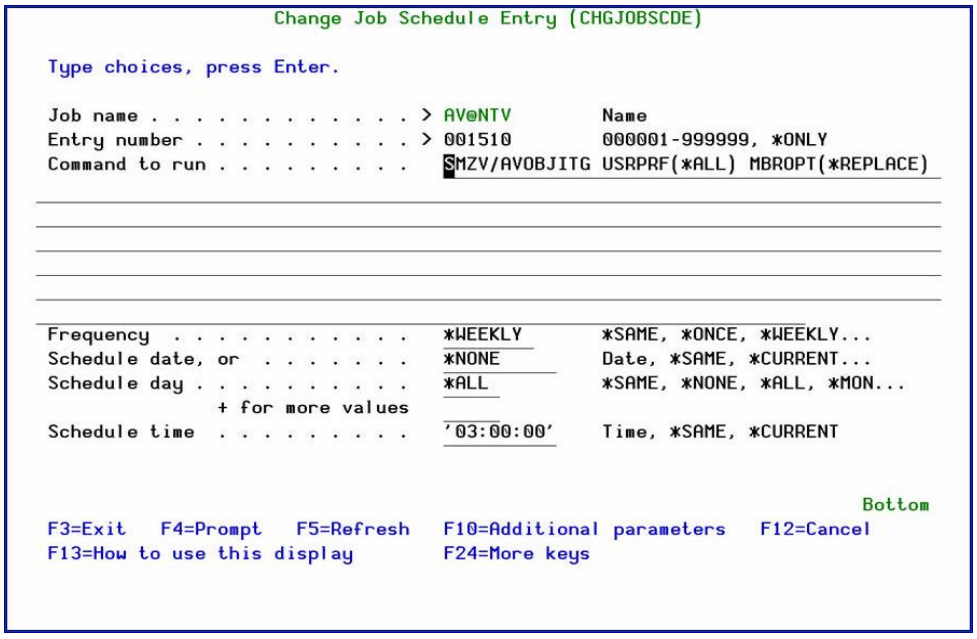
Submit Job

This option submits a batch job which runs the ***AVOBITG*** command. This info can either add information or delete it. This command, which exists in the ***SMZV*** library, runs the ***CHKOBJITG*** command and adds or replaces the existing collected data with the new. For a detailed description of all its parameters (except ****REPLACE*** and ****ADD***), see the ***CHKOBJITG*** definition in the IBM literature.

Scheduling Future Scans

Use this option to schedule a regularly-occurring scan, i.e. 9:00 every morning, or a single, specific scan to occur at a later date.

1. Select **15. Schedule Scan**. The **Change Job Schedule Entry (CHGJOBSCDE)** screen appears.
2. Press **Enter** to view all the parameters. The following shows an example.


Change Job Schedule Entry (CHGJOBSCDE)
Type choices, press Enter.
Job name . . . . . > AV@NTV Name
Entry number . . . . . > 001510 000001-999999, *ONLY
Command to run . . . . . SMZV/AVOBJITG USRPRF(*ALL) MBROPT(*REPLACE)
Frequency . . . . . *WEEKLY *SAME, *ONCE, *WEEKLY...
Schedule date, or . . . . . *NONE Date, *SAME, *CURRENT...
Schedule day . . . . . *ALL *SAME, *NONE, *ALL, *MON...
+ for more values
Schedule time . . . . . '03:00:00' Time, *SAME, *CURRENT
Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys

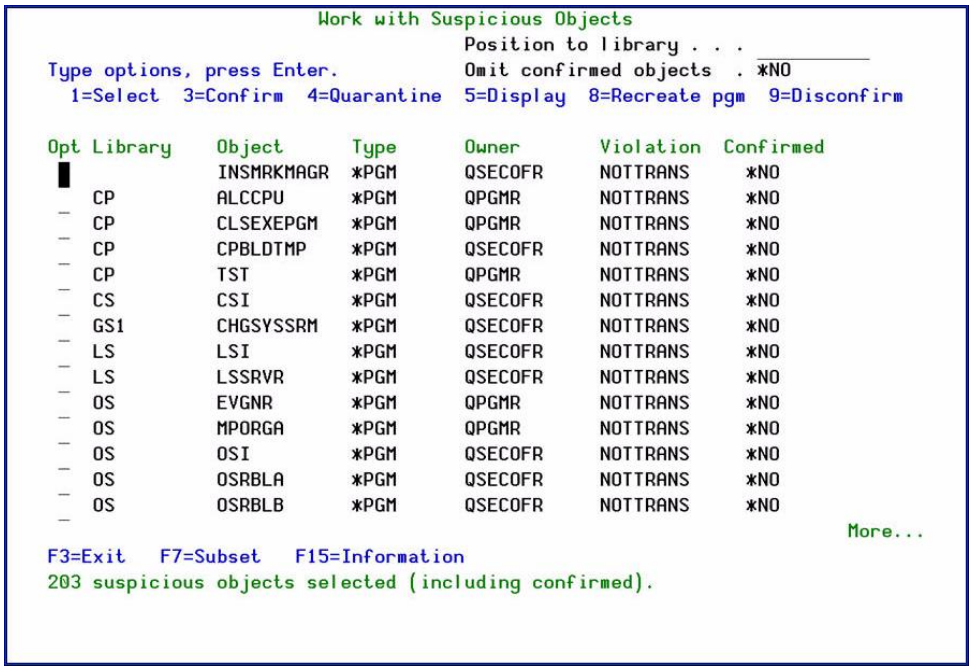
Change Job Schedule Entry (CHGJOBSCDE)

3. Enter your parameters (frequency, date, day, time) and press **Enter**.

Working with Suspicious Objects

To work with suspicious objects, follow this procedure.

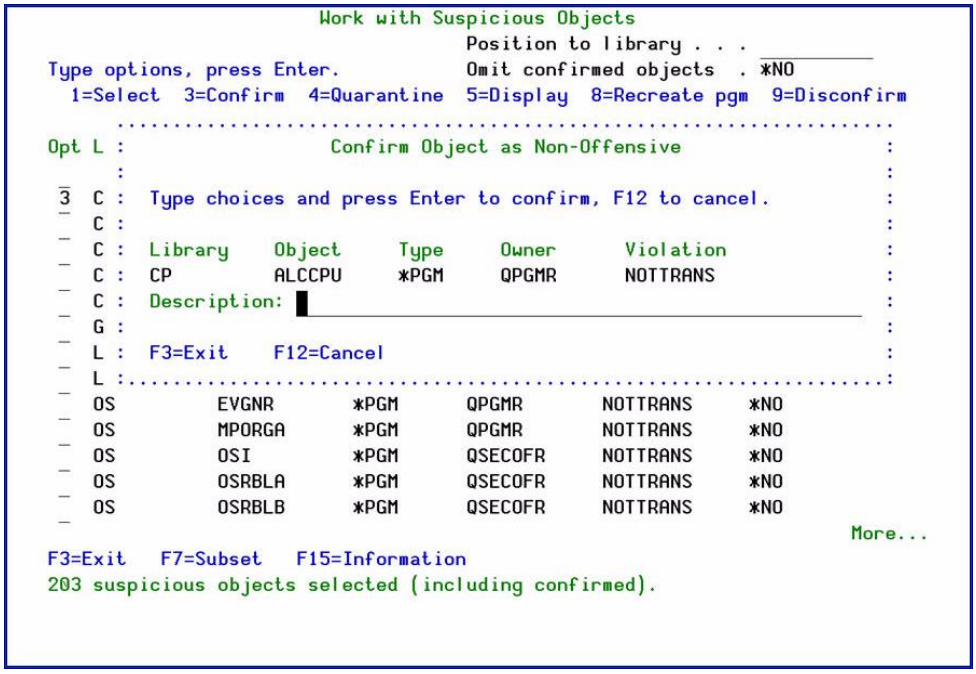
1. Select **21. Work with Suspicious Objects**. The **Work with Suspicious Objects screen** appears, showing those suspicious objects found by the scan.


Work with Suspicious Objects
Position to library . . .
Type options, press Enter.
Omit confirmed objects . *NO
1=Select 3=Confirm 4=Quarantine 5=Display 8=Recreate pgm 9=Disconfirm
Opt Library Object Type Owner Violation Confirmed
INSMRKMAGR *PGM QSECOFR NOTTRANS *NO
CP ALCCPU *PGM QPGMR NOTTRANS *NO
CP CLSEXEPGM *PGM QPGMR NOTTRANS *NO
CP CPBLDTMP *PGM QSECOFR NOTTRANS *NO
CP TST *PGM QPGMR NOTTRANS *NO
CS CSI *PGM QSECOFR NOTTRANS *NO
GS1 CHGSYSSRM *PGM QSECOFR NOTTRANS *NO
LS LSI *PGM QSECOFR NOTTRANS *NO
LS LSSRVR *PGM QSECOFR NOTTRANS *NO
OS EVGNR *PGM QPGMR NOTTRANS *NO
OS MPORGA *PGM QPGMR NOTTRANS *NO
OS OSI *PGM QSECOFR NOTTRANS *NO
OS OSRBLA *PGM QSECOFR NOTTRANS *NO
OS OSRBLB *PGM QSECOFR NOTTRANS *NO
More...
F3=Exit F7=Subset F15=Information
203 suspicious objects selected (including confirmed).

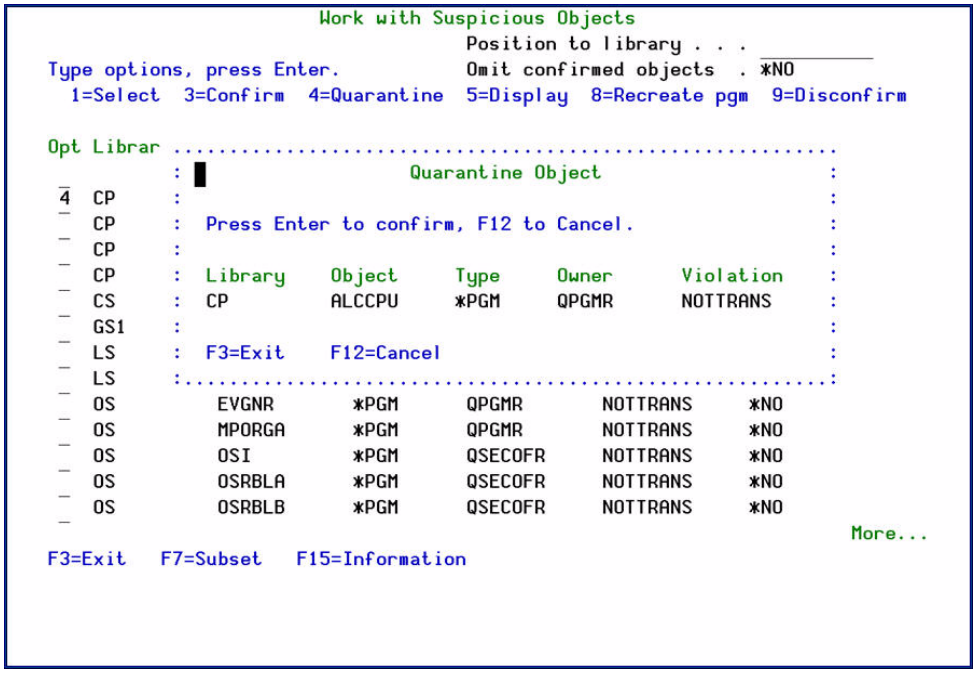
Work with Suspicious Objects

2. Choose one of the following options (screens are displayed following the table).

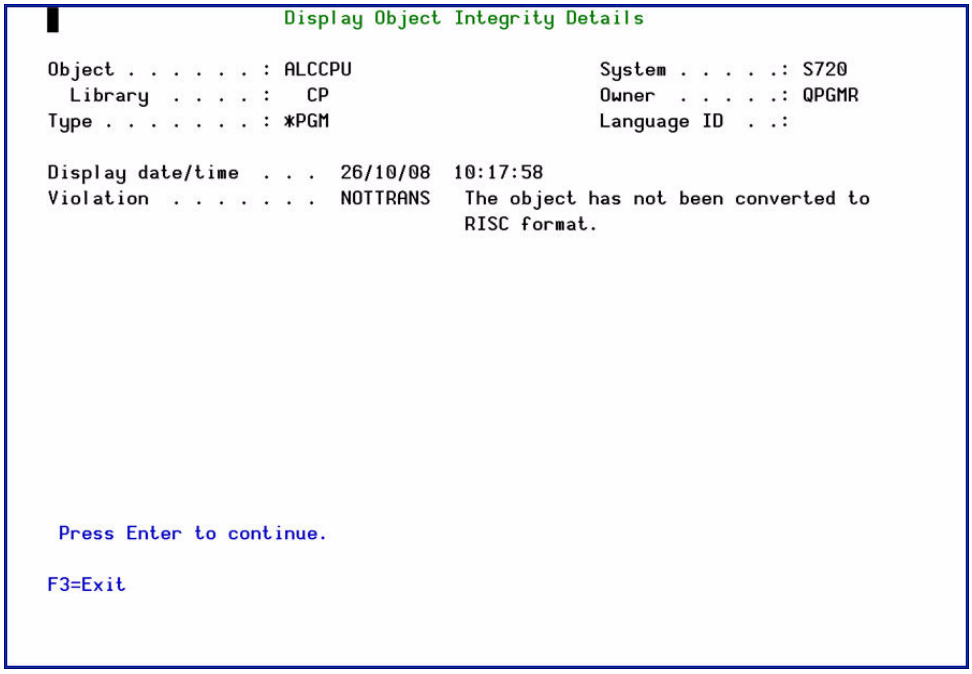
Option	Description
1 = Select	Displays details such as violation.
3 = Confirm	Confirms object as non-offensive. Enter descriptive text and press **Enter**.
4 = Quarantine	Places object in Quarantine.
5 = Display	Runs the appropriate display command as per the object type.
9 = Disconfirm	Removes the “non-offensive” status from a confirmed object.
F7 = Subset	Accesses the **Select Objects to Work With** screen. This enables you to determine which parameters appear on the **Work with Suspicious Objects** screen.


Work with Suspicious Objects
Position to library . . .
Type options, press Enter.
Omit confirmed objects . *NO
1=Select 3=Confirm 4=Quarantine 5=Display 8=Recreate pgm 9=Disconfirm
Opt L :
Confirm Object as Non-Offensive
3 C : Type choices and press Enter to confirm, F12 to cancel.
C :
C : Library Object Type Owner Violation
C : CP ALCCPU *PGM QPGMR NOTTRANS
C : Description:
G :
L : F3=Exit F12=Cancel
L :
OS EVGNR *PGM QPGMR NOTTRANS *NO
OS MPORGA *PGM QPGMR NOTTRANS *NO
OS OSI *PGM QSECOFR NOTTRANS *NO
OS OSRBLA *PGM QSECOFR NOTTRANS *NO
OS OSRBLB *PGM QSECOFR NOTTRANS *NO
More...
F3=Exit F7=Subset F15=Information
203 suspicious objects selected (including confirmed).

Work with Suspicious Objects: Confirm Object as Non-Offensive


Work with Suspicious Objects
Position to library . . .
Type options, press Enter.
Omit confirmed objects . *NO
1=Select 3=Confirm 4=Quarantine 5=Display 8=Recreate pgm 9=Disconfirm
Opt Librar
Quarantine Object
4 CP
CP Press Enter to confirm, F12 to Cancel.
CP
CP Library Object Type Owner Violation
CS CP ALCCPU *PGM QPGMR NOTTRANS
GS1
LS F3=Exit F12=Cancel
LS
OS EVGNR *PGM QPGMR NOTTRANS *NO
OS MPORGA *PGM QPGMR NOTTRANS *NO
OS OSI *PGM QSECOFR NOTTRANS *NO
OS OSRBLA *PGM QSECOFR NOTTRANS *NO
OS OSRBLB *PGM QSECOFR NOTTRANS *NO
More...
F3=Exit F7=Subset F15=Information

Work with Suspicious Objects: Quarantine Object


Display Object Integrity Details
Object . . . . . : ALCCPU
Library . . . . : CP
Type . . . . . : *PGM
System . . . . .: S720
Owner . . . . .: QPGMR
Language ID . .:
Display date/time . . . 26/10/08 10:17:58
Violation . . . . . NOTTRANS The object has not been converted to RISC format.
Press Enter to continue.
F3=Exit

Display Object Integrity Details (Option 1)

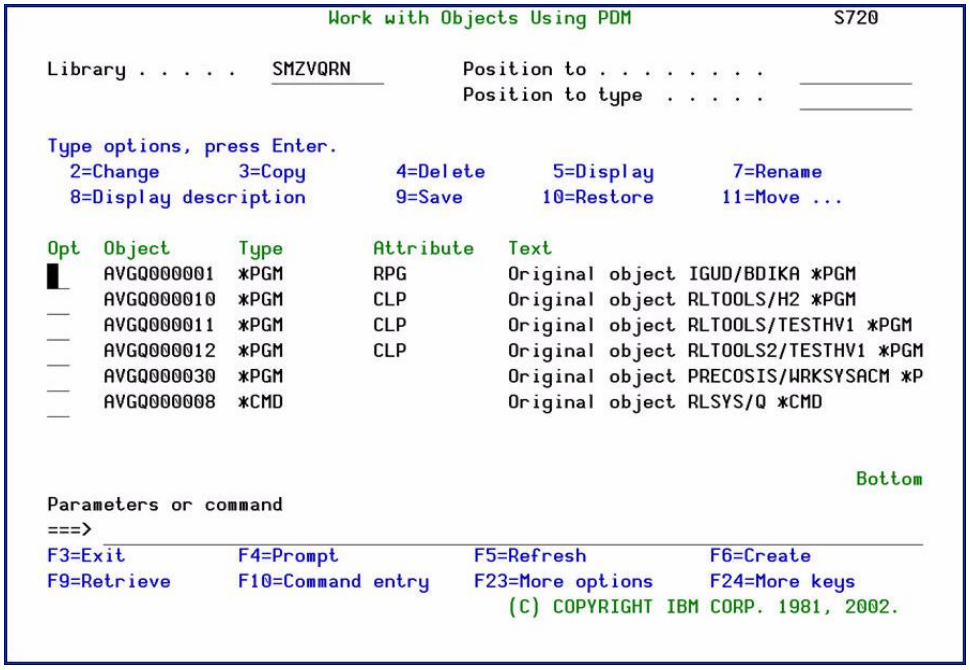
3. Type choices and/or press **Enter** to confirm.

Working with Quarantined Objects

An object placed in Quarantine is isolated and can do no further harm (see *Chapter Four* for details). After an object is placed in Quarantine, you can view details about that object, or delete it permanently. (See *Creating Reports* at the end of this chapter for information on reports)

To work with objects in Quarantine, follow this procedure.

1. Select **61. Work with Quarantined Objects**. The **Work with Objects Using PDM** screen appears.


Work with Objects Using PDM S720
Library . . . . . SMZVQRN
Position to . . . . . .
Position to type . . . . .
Type options, press Enter.
2=Change 3=Copy 4=Delete 5=Display 7=Rename
8=Display description 9=Save 10=Restore 11=Move ...
Opt Object Type Attribute Text
AVGQ000001 *PGM RPG Original object IGUD/BDIKA *PGM
AVGQ000010 *PGM CLP Original object RLTOOLS/H2 *PGM
AVGQ000011 *PGM CLP Original object RLTOOLS/TESTHV1 *PGM
AVGQ000012 *PGM CLP Original object RLTOOLS2/TESTHV1 *PGM
AVGQ000030 *PGM Original object PRECOSIS/WRKSYSACM *P
AVGQ000008 *CMD Original object RLSYS/Q *CMD
Bottom
Parameters or command
===>
F3=Exit F4=Prompt F5=Refresh F6=Create
F9=Retrieve F10=Command entry F23=More options F24=More keys
(C) COPYRIGHT IBM CORP. 1981, 2002.

Work With Objects Using PDM

2. Select **Opt 8** to display a description of the suspicious object or **Opt 4** to delete it permanently.

Creating Reports

Create reports to suit your needs by using the following options. Simply select the correct report type and then follow the wizard.

Creating Reports on Suspicious Objects

This feature runs reports on all suspicious objects, both confirmed and non-confirmed.

1. Select **Opt. 51. All Suspicious Objects**. The **Display AV Object Integrity** screen appears.
2. Leave options at default and press **Enter** to access the **Delay Suspicious Objects** screen. Choose one of the following options.

- Enter **Opt 1** to select an object. The **Display Object Integrity Details** screen appears.
- Press **F7** to access the **Select Objects to Work With** screen.

Creating Reports on all Non-Confirmed Objects

This feature runs reports on all non-confirmed suspicious objects.

1. Select **Opt. 52. All Suspicious Objects**. The **Display AV Object Integrity** screen appears.
2. Leave all options at their default parameters and press **Enter** to access the **Delay Suspicious Objects** screen. Choose one of the following options.
   - Enter **Opt 1** to select an object. The **Display Object Integrity Details** screen appears.
   - Press **F7** to access the **Select Objects to Work With** screen.

Creating Reports on all Confirmed Objects

This feature runs reports on all confirmed suspicious objects.

1. Select **Opt. 55. All Suspicious Objects**. The **Display AV Object Integrity** screen appears.
2. Leave all options at their default parameters and press **Enter** to access the **Display Confirmed Violation** screen. Choose one of the following options.

- Enter **Opt 1** to select an object. The **Display Confirmed Object Integrity Detail** screen appears.
- Press **F7** to access the **Select Objects to Work With** screen.

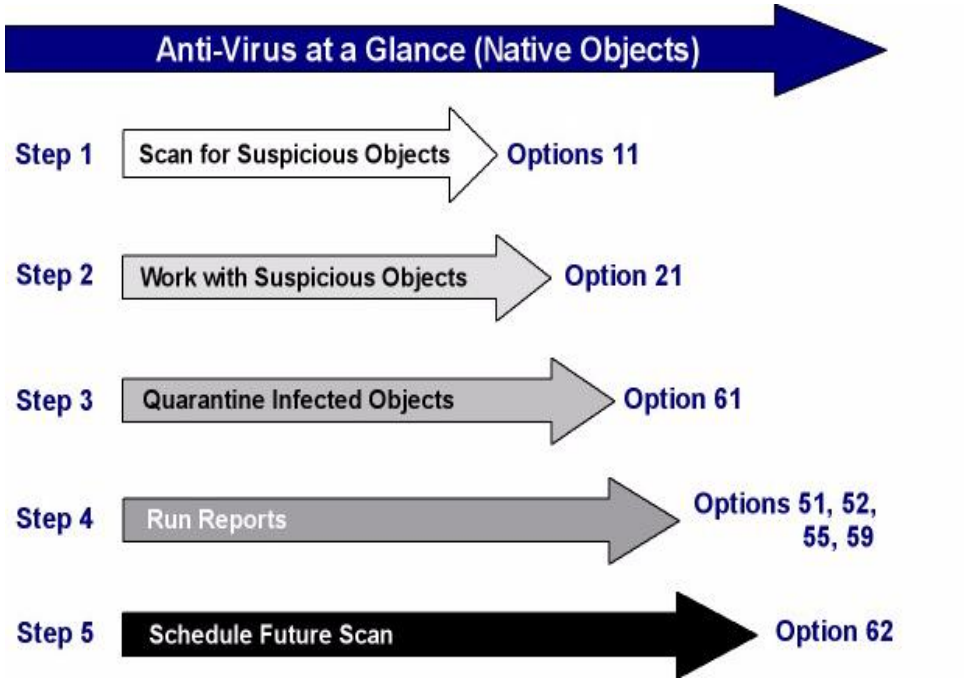
Create Reports on all Quarantined Objects

To run reports on objects found in Quarantine:

1. Select **Opt. 59. All Suspicious Objects**.
2. In the **Display Library** screen, select **Opt 5** to display the object's full attributes, and then press **Enter** to access the **Display Object Description - Full** screen.
3. Press **Enter** to return to the **Display Library** screen.

Anti-Virus at a Glance (Native Objects)

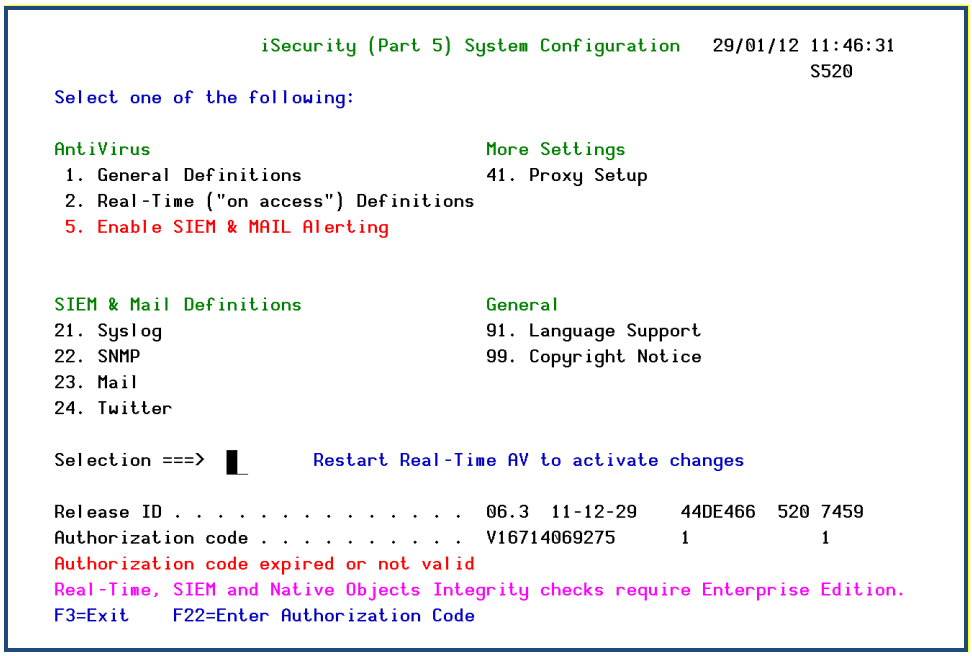
The following chart shows the basic procedures described in this chapter:



Chapter 4: System Configuration

Select option **81. System Configuration**

NOTE: *If system password is requested, type **QSECOFR.***

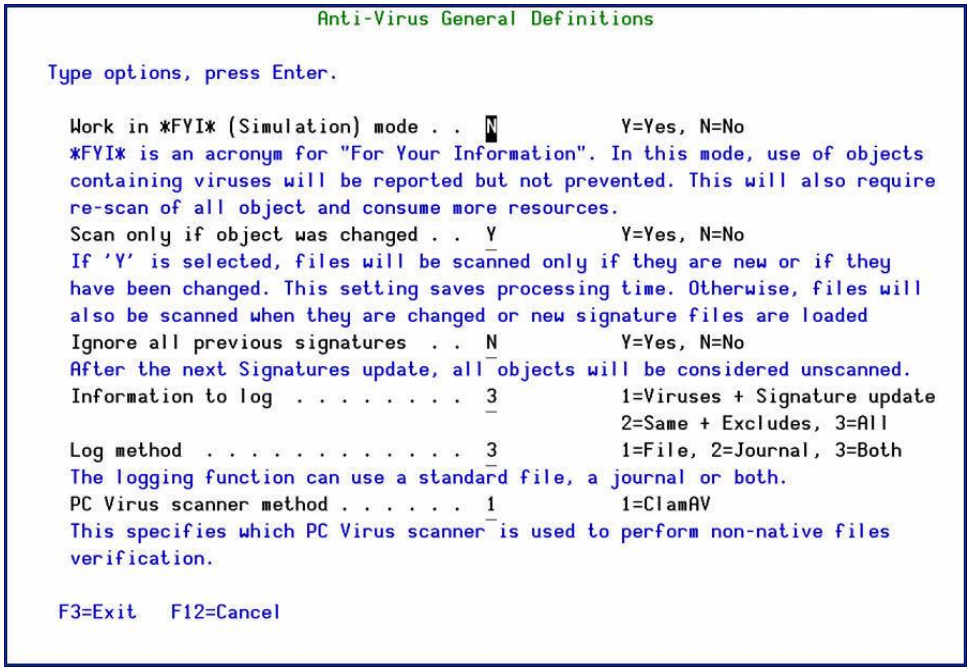

iSecurity (Part 5) System Configuration 29/01/12 11:46:31
S520
Select one of the following:
AntiVirus
1. General Definitions
2. Real-Time ("on access") Definitions
5. Enable SIEM & MAIL Alerting
More Settings
41. Proxy Setup
SIEM & Mail Definitions
21. Syslog
22. SNMP
23. Mail
24. Twitter
General
91. Language Support
99. Copyright Notice
Selection ===>
Restart Real-Time AV to activate changes
Release ID 06.3 11-12-29 44DE466 520 7459
Authorization code V16714069275 1 1
Authorization code expired or not valid
Real-Time, SIEM and Native Objects Integrity checks require Enterprise Edition.
F3=Exit F22=Enter Authorization Code

iSecurity (Part 5) System Configuration

General Definitions

This option presents general definitions relating to log and scans. Follow this procedure:

1. Select **1. General Definitions** from the **iSecurity (part 5) System Configuration** screen. The **Anti-Virus General Definitions** screen appears.
2. Set parameters and definitions according to the following table and press Enter.


Anti-Virus General Definitions
Type options, press Enter.
Work in *FYI* (Simulation) mode . . N Y=Yes, N=No
FYI is an acronym for "For Your Information". In this mode, use of objects
containing viruses will be reported but not prevented. This will also require
re-scan of all object and consume more resources.
Scan only if object was changed . . Y Y=Yes, N=No
If 'Y' is selected, files will be scanned only if they are new or if they
have been changed. This setting saves processing time. Otherwise, files will
also be scanned when they are changed or new signature files are loaded
Ignore all previous signatures . . N Y=Yes, N=No
After the next Signatures update, all objects will be considered unscanned.
Information to log . . . . . 3 1=Viruses + Signature update
2=Same + Excludes, 3=All
Log method . . . . . 3 1=File, 2=Journal, 3=Both
The logging function can use a standard file, a journal or both.
PC Virus scanner method . . . . . 1 1=ClamAV
This specifies which PC Virus scanner is used to perform non-native files
verification.
F3=Exit F12=Cancel

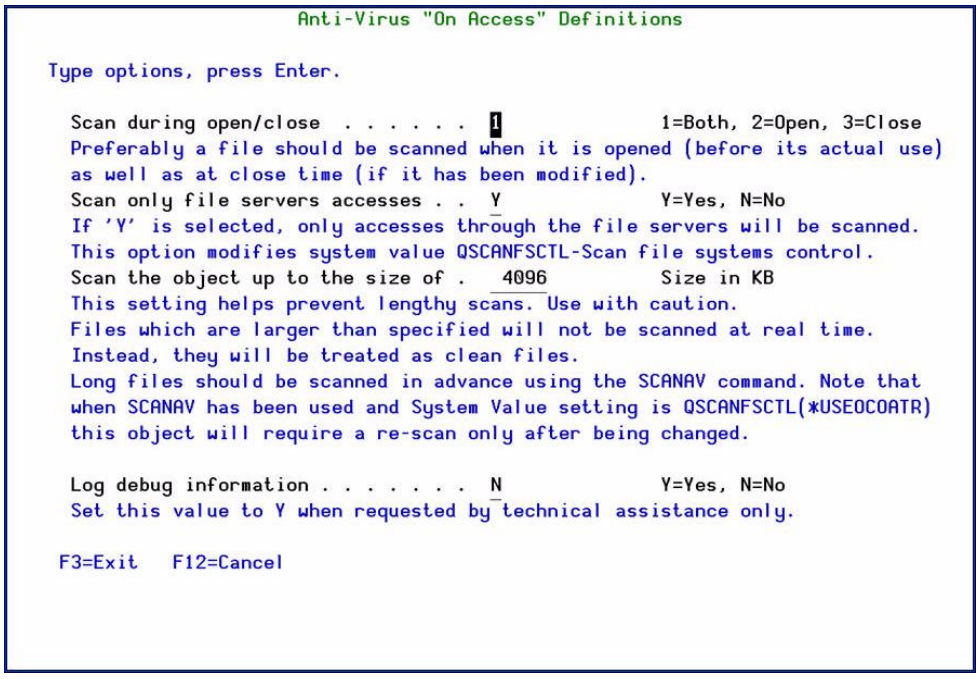
Anti-Virus General Definitions

Option	Description
Work in FYI Simulation Mode	The FYI Simulation Mode allows users to scan files without marking files as scanned. **Y** = Simulation mode – files not marked as scanned. **N** = Files are marked as scan failure (virus) or scan success (clean)
Scan only if object was changed	**Y** = Files will be scanned only if they are new or if they have been changed. This setting saves processing time. **N** = Files will be scanned when they are changed or new signature files are loaded
Ignore all previous signatures	After the next Signatures update, all objects will be considered un-scanned.
Information to log	**1** = Viruses + Signature update **2** = Same + Excludes **3** = All

Option	Description
Log method	The logging function can use a standard file, a journal or both **1** = Standard file **2** = Journal **3** = Both file and journal
PC Virus scanner method	Specifies which PC Virus scanner is used to perform IFS files scan. (Currently only ClamAV).

On Access Definitions

To set the scan definitions, select option **2. "On Access" Definitions.**


Anti-Virus "On Access" Definitions
Type options, press Enter.
Scan during open/close . . . . . 1 1=Both, 2=Open, 3=Close
Preferably a file should be scanned when it is opened (before its actual use)
as well as at close time (if it has been modified).
Scan only file servers accesses . . Y Y=Yes, N=No
If 'Y' is selected, only accesses through the file servers will be scanned.
This option modifies system value QSCANFSCTL-Scan file systems control.
Scan the object up to the size of . 4096 Size in KB
This setting helps prevent lengthy scans. Use with caution.
Files which are larger than specified will not be scanned at real time.
Instead, they will be treated as clean files.
Long files should be scanned in advance using the SCANAV command. Note that
when SCANAV has been used and System Value setting is QSCANFSCTL(*USEOCOATR)
this object will require a re-scan only after being changed.
Log debug information . . . . . N Y=Yes, N=No
Set this value to Y when requested by technical assistance only.
F3=Exit F12=Cancel

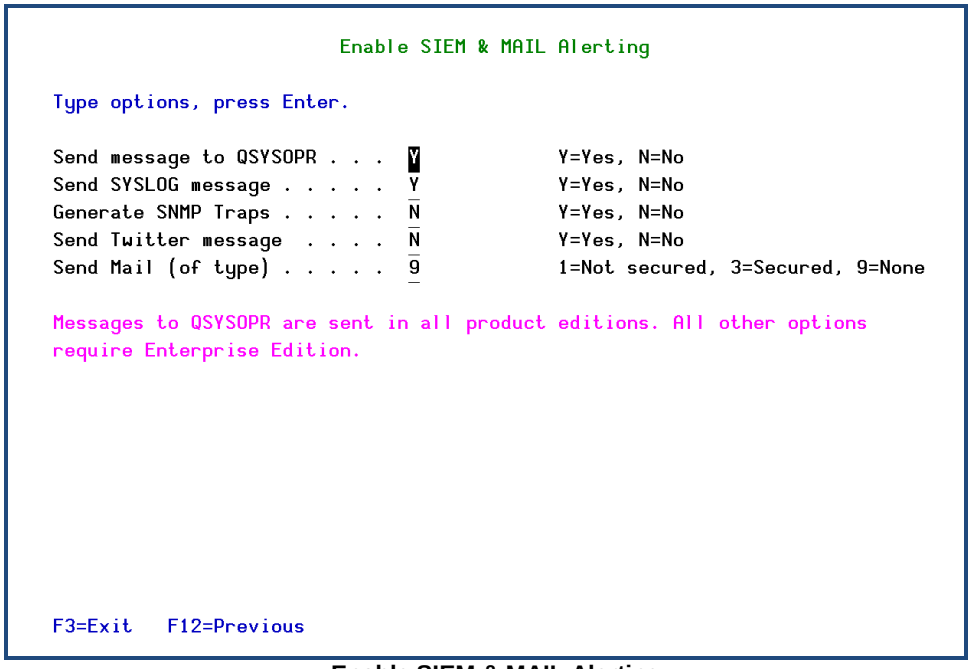
Anti-Virus "On Access" Definitions

Option	Description
Scan during open/close	It is recommended that files are scanned when opened, before their actual use, as well as when they are closed (if they have been modified). **1**=Both (recommended) **2**=Open **3**=Close

Option	Description
Scan only file servers accesses	This option modifies system value QSCANFSCTL-Scan file systems control **Y**=Yes, only access attempts carried out through the file servers **N**=No, scan from WRKLNK or EDITF as well.
Scan the object up to the size of...	Size in KB This setting helps prevent lengthy scans. Use with caution. Files which are larger than specified will not be scanned at real time, but a message will be inserted in the log file. Instead, they will be treated as clean files. Large files should be scanned in advance using the SCANAV command. Note that when SCANAV has been used and System Value setting is QSCANFSCTL(*USEOCOATR) this object will require a re-scan only after being changed.
Log debug information	**N**=No, default **Y**=Yes, set this value to Y when requested by technical assistance only

Enable SIEM & MAIL Alerting

From the **iSecurity (Part 5) System Configuration** screen, select option **5. Enable SIEM & MAIL Alerting** to send message alerts to QSYSOPR, E-mail address and SYSLOG.11

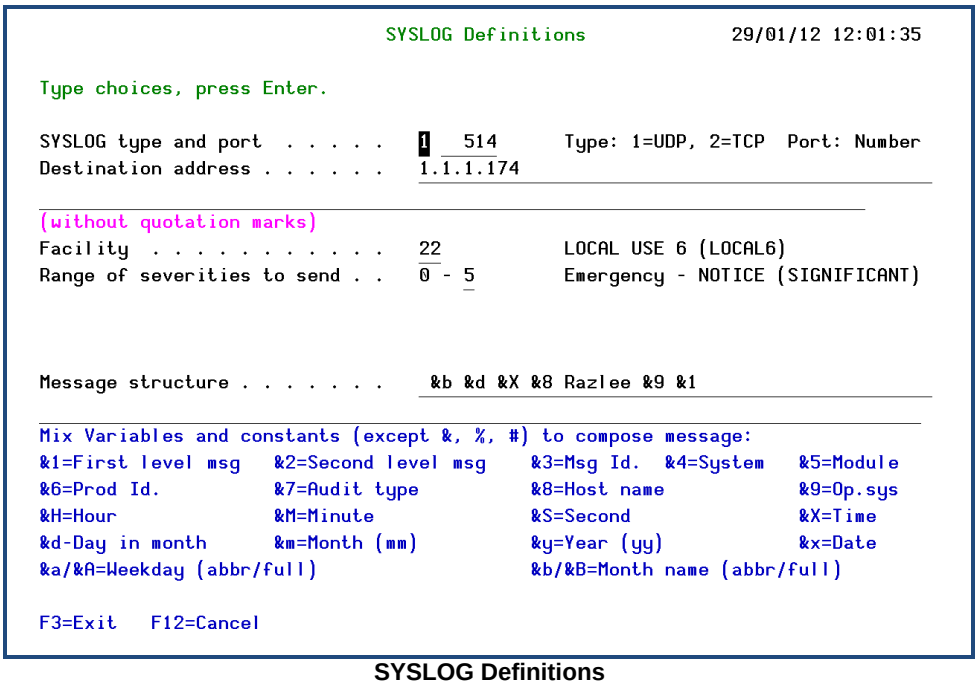

Enable SIEM & MAIL Alerting
Type options, press Enter.
Send message to QSYSOPR . . . Y Y=Yes, N=No
Send SYSLOG message . . . . . Y Y=Yes, N=No
Generate SNMP Traps . . . . . N Y=Yes, N=No
Send Twitter message . . . . N Y=Yes, N=No
Send Mail (of type) . . . . . 9 1=Not secured, 3=Secured, 9=None
Messages to QSYSOPR are sent in all product editions. All other options require Enterprise Edition.
F3=Exit F12=Previous

Enable SIEM & MAIL Alerting

SYSLOG Definitions

This feature sends different events from the AS/400 different facilities (such as logs and message systems) to a remote Syslog server according to range of severities like: emergency, alert, critical, error, warning and more.

Select option **21. Syslog** and define whether to send Syslog message, to what IP address, from which facility (list of optional facilities below), in what range of severity (list below) and how will the message look.


SYSLOG Definitions
29/01/12 12:01:35
Type choices, press Enter.
SYSLOG type and port . . . . . 1 514 Type: 1=UDP, 2=TCP Port: Number
Destination address 1.1.1.174
(without quotation marks)
Facility . . . . . 22 LOCAL USE 6 (LOCAL6)
Range of severities to send . . 0 - 5 Emergency - NOTICE (SIGNIFICANT)
Message structure . . . . . &b &d &X &8 Razlee &9 &1
Mix Variables and constants (except &, %, #) to compose message:
&1=First level msg &2=Second level msg &3=Msg Id. &4=System &5=Module
&6=Prod Id. &7=Audit type &8=Host name &9=Op.sys
&H=Hour &M=Minute &S=Second &X=Time
&d-Day in month &m=Month (mm) &y=Year (yy) &x=Date
&a/&A=Weekday (abbr/full) &b/&B=Month name (abbr/full)
F3=Exit F12=Cancel

SYSLOG Definitions

****SYSLFC - SYSLOG FACILITY:**

KERNEL MESSAGES	FTP DAEMON
USER-LEVEL MESSAGES	NTP SUBSYSTEM
MAIL SYSTEM	LOG AUDIT
SYSTEM DAEMONS	LOG ALERT
SECURITY/AUTHORIZATION	CLOCK DAEMON
MESSAGES	LOCAL USE 0 (LOCAL0)
SYSLOGD INTERNAL	LOCAL USE 1 (LOCAL1)
LINE PRINTER SUBSYSTEM	LOCAL USE 2 (LOCAL2)
NETWORK NEWS SUBSYSTEM	LOCAL USE 3 (LOCAL3)
UUCP SUBSYSTEM	LOCAL USE 4 (LOCAL4)
CLOCK DAEMON	LOCAL USE 5 (LOCAL5)
SECURITY/AUTHORIZATION	LOCAL USE 6 (LOCAL6)
MESSAGES	LOCAL USE 7 (LOCAL7)

****SYSLSV - SYSLOG SEVERITY:**

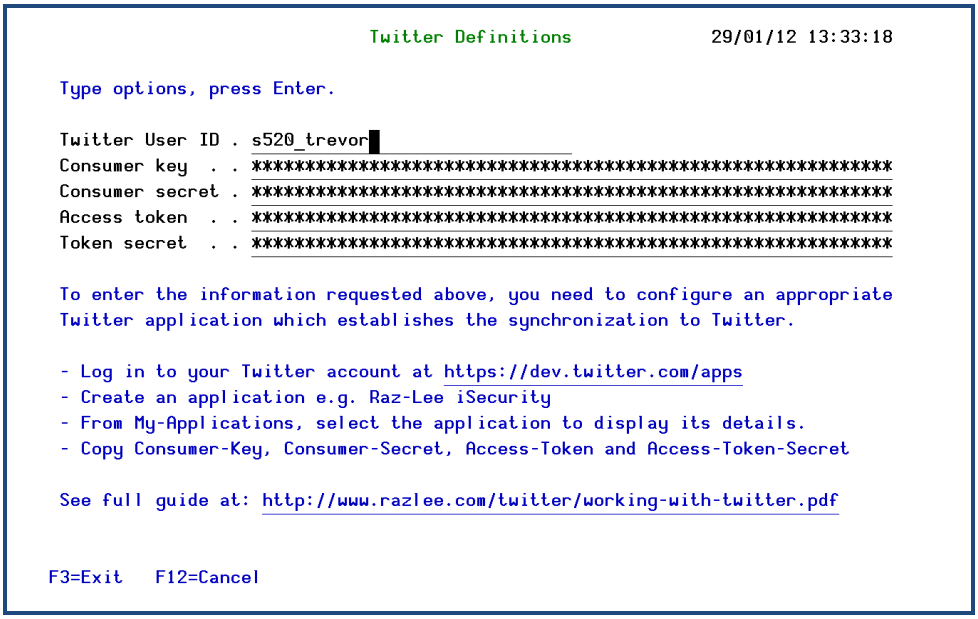
EMERGENCY	WARNING
ALERT	NOTICE (SIGNIFICANT)
CRITICAL	INFORMATIONAL
ERROR	DEBUG

SNMP Definitions

Select option **22. SNMP** to display the SNMP definitions. Use the following command text to define the SNMP Trap manager:
ADDTCPHTE INTNETADR(n.n.n.n) HOSTNAME(TRAPMAN).

Twitter Definitions

Select option **24. Twitter** to define the Twitter permissions for sending messages. For detailed instructions on defining Twitter for iSecurity Anti-Virus, see the following document: http://www.razlee.com/twitter/working-with-twitter.pdf.


Twitter Definitions
29/01/12 13:33:18
Type options, press Enter.
Twitter User ID . s520_trevor
Consumer key . .
Consumer secret .
Access token . .
Token secret . .
To enter the information requested above, you need to configure an appropriate
Twitter application which establishes the synchronization to Twitter.
- Log in to your Twitter account at https://dev.twitter.com/apps
- Create an application e.g. Raz-Lee iSecurity
- From My-Applications, select the application to display its details.
- Copy Consumer-Key, Consumer-Secret, Access-Token and Access-Token-Secret
See full guide at: http://www.razlee.com/twitter/working-with-twitter.pdf
F3=Exit F12=Cancel

Twitter Definitions

A

Appendix: License Agreement

GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below. When we speak of free software, we are referring to freedom of use,not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it. For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library. To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license. Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated

libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library. We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library. The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you". A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification").

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. The modified work must itself be a software library.
   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.
4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.
5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License. However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. 16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS